Posting description/title	Link	Date posted on ICOTR	Document orig. year	Subject matter category (used in charts)	Subcat.
Letter from Former Deputy Assistant Attorney General Yoo to former FISC Presiding Judge Kollar-Kotelly	https://www.dni.gov/files/documents/OLC%209-with%20attachment.pdf	2/29/2016	2002	PSP	
President's Surveillance Program Volume IA	https://www.dni.gov/files/documents/921/PSPvolIA.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IB	https://www.dni.gov/files/documents/921/PSPvolIB.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IC	https://www.dni.gov/files/documents/921/PSPvolIC.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIA	https://www.dni.gov/files/documents/921/PSPvolIIA.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIB	https://www.dni.gov/files/documents/921/PSPvolIIB.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIC	https://www.dni.gov/files/documents/921/PSPvolIIC.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IID	https://www.dni.gov/files/documents/921/PSPvolIID.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIE	https://www.dni.gov/files/documents/921/PSPvolIIE.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIF	https://www.dni.gov/files/documents/921/PSPvolIIF.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIG	https://www.dni.gov/files/documents/921/PSPvolIIG.pdf	9/21/2015	2009	PSP	

President's Surveillance Program Volume IIIA	https://www.dni.gov/files/documents/921/PSPvolIIIA.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIIB	https://www.dni.gov/files/documents/921/PSPvolIIIB.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIIC	https://www.dni.gov/files/documents/921/PSPvolIIIC.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIID	https://www.dni.gov/files/documents/921/PSPvolIIID.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIIE	https://www.dni.gov/files/documents/921/PSPvolIIIE.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIIF	https://www.dni.gov/files/documents/921/PSPvolIIIF.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIIG	https://www.dni.gov/files/documents/921/PSPvolIIIG.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIIH	https://www.dni.gov/files/documents/921/PSPvolIIIH.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIII	https://www.dni.gov/files/documents/921/PSPvolIIII.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIIJ	https://www.dni.gov/files/documents/921/PSPvolIIIJ.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIIK	https://www.dni.gov/files/documents/921/PSPvolIIIK.pdf	9/21/2015	2009	PSP	
President's Surveillance Program Volume IIIL	https://www.dni.gov/files/documents/921/PSPvolIIIL.pdf	9/21/2015	2009	PSP	

2009 Joint IG Report on the PSP Annex volume 3 part 6	24/2009%20Joint%20IG%20Report%20on%20the%20PSP_Annex%20Vol.%20III-F.pdf	5/1/2015	2009	PSP	
Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2014 (dated 4/22/15)	http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014	4/25/2015	2009	PSP	
2009 Joint IG Report on the PSP Vol. I	https://www.dni.gov/files/documents/424/2009%20Joint%20IG%20Report%20on%20the%20PSP%20Vol.%20I.pdf	4/25/2015	2009	PSP	
2009 Joint IG Report on the PSP Annex volume 2 part 1	https://www.dni.gov/files/documents/424/2009%20Joint%20IG%20Report%20on%20the%20PSP_Annex%20Vol.%20II-A.pdf	4/25/2015	2009	PSP	
2009 Joint IG Report on the PSP Annex volume 2 part 2	24/2009%20Joint%20IG%20Report%20on%20the%20PSP_Annex%20Vol.%20II-B.pdf	4/25/2015	2009	PSP	
2009 Joint IG Report on the PSP Annex volume 2 part 3	24/2009%20Joint%20IG%20Report%20on%20the%20PSP_Annex%20Vol.%20II-C.pdf	4/25/2015	2009	PSP	
2009 Joint IG Report on the PSP Annex volume 3 part 1	24/2009%20Joint%20IG%20Report%20on%20the%20PSP_Annex%20Vol.%20III-A.pdf	4/25/2015	2009	PSP	
2009 Joint IG Report on the PSP Annex volume 3 part 2	24/2009%20Joint%20IG%20Report%20on%20the%20PSP_Annex%20Vol.%20III-B.pdf	4/25/2015	2009	PSP	
2009 Joint IG Report on the PSP Annex volume 3 part 3	24/2009%20Joint%20IG%20Report%20on%20the%20PSP_Annex%20Vol.%20III-C.pdf	4/25/2015	2009	PSP	
2009 Joint IG Report on the PSP Annex volume 3 part 4	24/2009%20Joint%20IG%20Report%20on%20the%20PSP_Annex%20Vol.%20III-D.pdf	4/25/2015	2009	PSP	
2009 Joint IG Report on the PSP Annex volume 3 part 5	24/2009%20Joint%20IG%20Report%20on%20the%20PSP_Annex%20Vol.%20III-E.pdf	4/25/2015	2009	PSP	
NSA Alexander 2007 MCI & Verizon Declaration	505/NSA%20Alexander%202007%20Declassified%20Verizon%20Declaration.pdf	5/6/2014	2007	PSP	

U.S. Department of Justice

Office of Legal Counsel

Office of the Deputy Assistant Attorney General

Washington, D.C. 20530

May 17, 2002

Judge Colleen Kollar-Kotelly
U.S. District Court for the District of Court
U.S. Courthouse
3d & Constitution Ave., N.W.
Washington, D.C. 20001

Dear Judge:

It was a pleasure to meet you today. I am writing this letter, at the direction of the Attorney General and in the interests of comity between the executive and legislative branches, to follow up on your questions concerning the scope of the President's authority to conduct warrantless searches. In particular, this letter discusses the President's power to deploy expanded electronic surveillance techniques in response to the terrorist attacks against the United States on September 11, 2001. This letter outlines the legal justifications for such surveillance, which could be conducted without a warrant for national security purposes. Under the current circumstances, in which international terrorist groups continue to pose an immediate threat, we have concluded that such surveillance would be reasonable under the Fourth Amendment because it advances the compelling government interest of protecting the Nation from direct attack.

Part I of this memorandum discusses the relevant factual background. Part II examines the legal framework that governs the collection of electronic communications in the United States, and whether warrantless electronic surveillance is consistent with it. Part III reviews different doctrines that affect the legality of different types of surveillance. Part IV discusses the application of the Fourth Amendment in light of the September 11 attacks.

I.

Four coordinated terrorist attacks took place in rapid succession on the morning of September 11, 2001, aimed at critical Government buildings in the Nation's capital and landmark buildings in its financial center. Terrorists hijacked four airplanes: one then crashed into the Pentagon and two in the World Trade Center towers in New York City; the fourth, which was headed towards Washington, D.C., crashed in

Pennsylvania after passengers attempted to regain control of the aircraft. The attacks caused about five thousand deaths and thousands more injuries. Air traffic and communications within the United States have been disrupted; national stock exchanges were shut for several days; damage from the attack has been estimated to run into the billions of dollars. The President has found that these attacks are part of a violent terrorist campaign against the United States by groups affiliated with Al-Qaeda, an organization headed by Usama bin Laden, that includes the suicide bombing attack on the U.S.S. Cole in 2000, the bombing of our embassies in Kenya and Tanzania in 1998, the attack on a U.S. military housing complex in Saudi Arabia in 1996, and the bombing of the World Trade Center in 1993. The nation has undergone an attack using biological weapons, in which unknown terrorists have sent letters containing anthrax to government and media facilities, and which have resulted in the closure of executive, legislative, and judicial branch buildings.

In response, the Government has engaged in a broad effort at home and abroad to counter terrorism. Pursuant to his authorities as Commander-in-Chief and Chief Executive, the President has ordered the Armed Forces to attack al-Qaeda personnel and assets in Afghanistan, and the Taliban militia that harbors them. Congress has provided its support for the use of force against those linked to the September 11, 2001 attacks, and has recognized the President's constitutional power to use force to prevent and deter future attacks both within and outside the United States. S.J. Res. 23, Pub. L. No. 107-40, 115 Stat. 224 (2001). The military has also been deployed domestically to protect sensitive government buildings and public places from further terrorist attack. The Justice Department and the FBI have launched a sweeping investigation in response to the September 11 attacks. In October, 2001, Congress enacted legislation to expand the Justice Department's powers of surveillance against terrorists. By executive order, the President has created a new office for homeland security within the White House to coordinate the domestic program against terrorism.

Electronic surveillance techniques would be part of this effort. The President would order warrantless surveillance in order to gather intelligence that would be used to prevent and deter future attacks on the United States. Given that the September 11 attacks were launched and carried out from within the United States itself, an effective surveillance program might include individuals and communications within the continental United States. This would be novel in two respects. Without access to any non-public sources, it is our understanding that generally the National Security Agency (NSA) only conducts electronic surveillance of communications outside the United States that do not involve United States persons. Usually, surveillance of communications by United States persons within the United States is conducted by the FBI pursuant to a warrant obtained under the Foreign Intelligence Surveillance Act ("FISA"). Second, interception could include electronic messages carried through the internet, which again could include communications within the United States involving United States persons. Currently, it is our understanding that neither the NSA nor law enforcement conducts broad monitoring of electronic communications in this manner within the United States, without specific authorization under FISA.

II.

This Part discusses the legal authorities that govern the intelligence agencies, and whether warrantless electronic surveillance is consistent with them. Section A concludes that while certain aspects of such electronic surveillance might be inconsistent with earlier executive order, a presidential decision to conduct the surveillance constitutes a legitimate waiver to the order and is not unlawful. Section B concludes that the Foreign Intelligence Surveillance Act ("FISA") does not restrict the constitutional authority of the executive branch to conduct surveillance of the type at issue here.

A.

The NSA was formed in 1952 by President Truman as part of the Defense Department. Under Executive Order 12,333, 46 Fed. Reg. 59941 (1981), the NSA is solely responsible for "signals intelligence activities ["SIGINT"]." Id. § 1.12(b)(1). It provides intelligence information acquired through the interception of communications to the White House, executive branch agencies, the intelligence community, and the armed forces for intelligence, counter-intelligence, and military purposes. Clearly, the basic authority for the establishment of the NSA is constitutional: the collections of SIGINT is an important part of the Commander-in-Chief and Chief Executive powers, which enable the President to defend the national security both at home and abroad. While Congress has enacted statutes authorizing the funding and organization of the NSA, it has never established any detailed statutory charter governing the NSA's activities. *See* Intelligence Authorization Act for FY 1993, Pub. L. No. 102-496, sec. 705 (giving Secretary of Defense responsibility to ensure, through the NSA, the "continued operation of an effective unified organization for the conduct of signals intelligence activities").

The NSA generally has limited its operations to the interception of international communications in which no United States person (a United States citizen, permanent resident alien, a U.S. corporation, or an unincorporated association with a substantial number of members who are U.S. citizens or permanent resident aliens) is a participant. According to publicly-available information, the NSA pulls in a great mass of international telephone, radio, computer, and other electronic communications, and then filters them using powerful computer systems for certain words or phrases. *See, e.g., Halkin v. Helms*, 690 F.2d 977, 983-84 (D.C. Cir. 1982). Congress, however, has not imposed any express statutory restrictions on the NSA's ability to intercept communications that involve United States citizens or that occur domestically. This lack of limitations can be further inferred from the National Security Act of 1947. The Act places a clear prohibition, for example, upon the Central Intelligence Agency's domestic activities. While Section 103 of the National Security Act commands the Director of Central Intelligence to "collect intelligence through human sources and by other appropriate means," it also adds "except that the Agency shall have no police, subpoena, or law enforcement powers or internal security functions." 50 U.S.C. § 403-3(d)(1) (1994 & Supp. V 1999). There is no similar provision that applies to the NSA, which implies that the NSA can conduct SIGINT operations domestically.

Rather than from statute, the limitation on the NSA's domestic SIGINT capabilities derives from executive order. Executive Order 12,333 requires that any "[c]ollection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the FBI." Executive Order 12,333, at § 2.3(b). If "significant foreign intelligence is sought," the Executive Order permits other agencies within the intelligence community to collect information "provided that no foreign intelligence collection by such agencies may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons." *Id*. Section 2.4 further makes clear that the intelligence community cannot use electronic surveillance, among other techniques, "within the United States or directed against United States persons abroad" unless they are according to procedures established by the agency head and approved by the Attorney General. In its own internal regulations, the NSA apparently has interpreted these provision as limiting its SIGINT operations only to international communications that do not involve United States persons.

Thus, the question arises whether a presidential decision to conduct warrantless electronic surveillance, for national security purposes, violates Executive Order 12,333, if such surveillance is not limited only to foreign communications that do not involve U.S. citizens. Thus, for example, all communications between United States persons, whether in the United States or not, and individuals in [redacted] might be intercepted. The President might direct the NSA to intercept communications between suspected terrorists, even if one of the parties is a United States person and the communication takes place between the United States and abroad. The non-content portion of electronic mail communications also might be intercepted, even if one of parties is within the United States, or one or both of the parties are non-citizen U.S. persons (i.e., a permanent resident alien). Such operations would expand the NSA's functions beyond the monitoring only of international communications of non-U.S. persons.

B1
B3

While such surveillance may go well beyond the NSA's current operations, it would not violate the text of the Executive Order. Executive Order 12,333 states that "when significant foreign intelligence is sought," the NSA and other agencies of the intelligence community may collect foreign intelligence within the United States. The only qualification on domestic collection is that it cannot be undertaken to acquire information about the domestic activities of United States persons. If United States persons were engaged in terrorist activities, either by communicating with members of Al Qaeda [redacted] or by communicating with foreign terrorists even within the United States, they are not engaging in purely "domestic" activities. Instead, they are participating in foreign terrorist activities that have a component within the United States. We do not believe that Executive Order 12,333 was intended to prohibit intelligence agencies from tracking international terrorist activities, solely because terrorists conduct those activities within the United States. This would create the odd incentive of providing international terrorists with more freedom to conduct their illegal activities *inside* the United States than outside of it. Rather, the Executive Order was meant to protect the privacy of United States persons where foreign threats were not involved. Further, Section 2.4 of Executive Order 12,333 contemplates that the NSA and other

B1
B3

intelligence agencies can collect intelligence within the United States, so long as the Attorney General approves the procedures.

Even if surveillance were to conflicts with Executive Order 12,333, it could not be said to be illegal. An executive order is only the expression of the President's exercise of his inherent constitutional powers. Thus, an executive order cannot limit a President, just as one President cannot legally bind future Presidents in areas of the executive's Article II authority. Further, there is no constitutional requirement that a President issue a new executive order whenever he wishes to depart from the terms of a previous executive order. In exercising his constitutional or delegated statutory powers, the President often must issue instructions to his subordinates in the executive branch, which takes the form of an executive order. An executive order, in no sense then, represents a command from the President to himself, and therefore an executive order does not commit the President himself to a certain course of action. Rather than "violate" an executive order, the President in authorizing a departure from an executive order has instead modified or waived it. Memorandum for the Attorney General, From: Charles J. Cooper, Assistant Attorney General, *Re: Legal Authority for Recent Covert Arms Transfers to Iran* (Dec. 17, 1986). In doing so, he need not issue a new executive order, rescind the previous order, or even make his waiver or suspension of the order publicly known. Thus, here, the October 4, 2001 Authorization, even if in tension with Executive Order 12,333, only represents a one-time modification or waiver of the executive order, rather than a "violation" that is in some way illegal.

B.

Although it would not violate either the statutory authority for the NSA's operations or Executive Order 12,333, warrantless electronic surveillance within the United States, for national security purposes, would be in tension with FISA. FISA generally requires that the Justice Department obtain a warrant before engaging in electronic surveillance within the United States, albeit according to lower standards than apply to normal law enforcement warrants. Indeed, some elements of an electronic surveillance program – such as intercepting the communications of individuals for which probable cause exists to believe are terrorists – could probably be conducted pursuant to a FISA warrant. Here, however, a national security surveillance program could be inconsistent with the need for secrecy, nor would it be likely that a court could grant a warrant for other elements of a surveillance program, such as the monitoring of all calls to and from a foreign nation, or the general collection of communication addressing information. Nonetheless, as our Office has advised before, and as the Justice Department represented to Congress during passage of the Patriot Act of 2001, which resulted in several amendment to FISA, FISA only provides a safe harbor for electronic surveillance, and cannot restrict the President's ability to engage in warrantless searches that protect the national security. Memorandum for David S. Kris, Associate Deputy Attorney General, from John C. Yoo, Deputy Assistant Attorney General, *Re: Constitutionality of Amending Foreign Intelligence Surveillance Act to Change the "Purpose" Standard for Searches* (Sept. 25, 2001). The

ultimate test of the October 4 Authorization, therefore, is not FISA but the Fourth Amendment itself.

FISA requires that in order to conduct electronic surveillance for foreign intelligence purposes, the Attorney General must approve an application for a warrant, which is then presented to a special Article III court. If the target of the surveillance is a foreign power, the application need not detail the communications sought or the methods to be used. If the target is an agent of a foreign power, which the statute defines to include someone who engages in international terrorism, 50 U.S.C. § 1801(b)(2)(C) (1994 & Supp. V 1999), the application must contain detailed information concerning the target's identity, the places to be monitored, the communications sought, and the methods to be used. *Id.* at § 1804(a)(3)-(11). After passage of the FISA amendments as part of the Patriot Act, the National Security Adviser must certify that a "significant" purpose of the surveillance is to obtain foreign intelligence information that cannot be obtained through normal investigative techniques. FISA defines foreign intelligence information to include information that relates to "actual or potential attack or other grave hostile acts of a foreign power" or its agent, or information concerning "sabotage or international terrorism" by a foreign power or its agent, or information that, if a United States person is involved, is necessary for the national security or conduct of foreign affairs. *Id.* at § 1801(e).

FISA provides more secrecy and a lower level of proof for warrants. FISA creates a lesser standard than required by the Fourth Amendment for domestic law enforcement warrants, because the Attorney General need not demonstrate probable cause of a crime. He must only show that there is reason to believe that the target is a foreign power or an agent of a foreign power, and that the places to be monitored will be used by them. *Id.* at § 1804(a)(4)(A)-(B). If the target is a United States person, however, the Court must find that the National Security Adviser's certification is not clearly erroneous.

We do not believe an electronic surveillance program, undertaken in response to the September 11, 2001 attacks, could fully satisfy FISA standards. Such a program could seek to intercept all communications between the United States and certain countries where terrorist groups are known to operate, or communications that involve terrorists as participants. An effective surveillance program might not be able to enforce a distinction between United States persons or aliens, or to require that there be any actual knowledge of the identity of the targets of the search. FISA, however, requires that the warrant application identify the target with some particularity, probably either by name or by pseudonym. *Id.* at § 1804(a)(3); *cf. United States v. Principie*, 531 F.2d 1132 (2d Cir. 1976). To the extent that a presidential order would require probable cause to believe that a participant in a communication is a terrorist, this would more than meet FISA standards that the Justice Department show that the subject of a search is an agent of a foreign power. A standard based on reasonable grounds also would probably meet FISA standards. This, however, would not save a surveillance program's interception of all communications between the United States and another country from statutory difficulties.

Further problems are presented by FISA's requirement that the application describe the "places"

or "facilities" that are to be used by the foreign agent. While this requirement clearly extends beyond specific communication nodes, such as phones, to include facilities, we believe it unlikely that FISA would allow surveillance [redacted] Title III of the 1968 Act, for example, also requires the specification of "facilities" in addition to "places," and defines them as devices that transmit communications between two points. The courts have read "facilities" to allow surveillance of multiple telephone lines, rather than just an individual phone. We have not found an example, however, in which a court has granted a Title III warrant that would cover [redacted] which is the object of the surveillance program contemplated here. Thus, it is unlikely that the FISA court would grant a warrant that could authorize an effective surveillance program undertaken in response to the September 11 attacks.

B1
B3

B1
B3

FISA purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence, just as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, claims to be the exclusive method for authorizing domestic electronic surveillance for law enforcement purposes. FISA establishes criminal and civil sanctions for anyone who engages in electronic surveillance, under color of law, except as authorized by statute, warrant, or court order. 50 U.S.C. § 1809-10. It might be thought, therefore, that a warrantless surveillance program, even if undertaken to protect the national security, would violate FISA's criminal and civil liability provisions.

Such a reading of FISA would be an unconstitutional infringement on the President's Article II authorities. FISA can regulate foreign intelligence surveillance only to the extent permitted by the Constitution's enumeration of congressional authority and the separation of powers. FISA itself is not required by the Constitution, nor does it necessarily establish standards and procedures that exactly match those required by the Fourth Amendment. Memorandum for David S. Kris, Associate Deputy Attorney General, from John C. Yoo, Deputy Assistant Attorney General, *Re: Constitutionality of Amending Foreign Intelligence Surveillance Act to Change the "Purpose" Standard for Searches* (Sept. 25, 2001); *cf.* Memorandum for Michael Vatis, Deputy Director, Executive Office for National Security, from Walter Dellinger, Assistant Attorney General, *Re: Standards for Searches Under Foreign Intelligence Surveillance Act* (Feb. 14, 1995). Instead, like the warrant process in the normal criminal context, FISA represents a statutory procedure that creates a safe harbor for surveillance for foreign intelligence purposes. If the government obtains a FISA warrant, its surveillance will be presumptively reasonable under the Fourth Amendment. Nonetheless, as we explained to Congress during passage of the Patriot Act, the ultimate test of whether the government may engage in foreign surveillance is whether the government's conduct is consistent with the Fourth Amendment, not whether it meets FISA.

This is especially the case where, as here, the executive branch possess the inherent constitutional power to conduct warrantless searches for national security purposes. Well before FISA's enactment, Presidents have consistently asserted – and exercised – their constitutional authority to conduct warrantless

searches necessary to protect the national security.[1] This Office has maintained, across different administrations controlled by different political parties, that the President's constitutional responsibility to defend the nation from foreign attack implies an inherent power to conduct warrantless searches. In 1995, we justified warrantless national security searches by recognizing that the executive branch needed flexibility in conducting foreign intelligence operations. Memorandum for Michael Vatis, Deputy Director, Executive Office for National Security, from Walter Dellinger, Assistant Attorney General, *Re: Standards for Searches Under Foreign Intelligence Surveillance Act* (Feb. 14, 1995). In 1980, we also said that "the lower courts – as well as this Department – have frequently concluded that authority does exist in the President to authorize such searches regardless of whether the courts also have the power to issue warrants for those searches. Memorandum for the Attorney General, from John M. Harmon, Assistant Attorney General, *Re: Inherent Authority* at 1 (Oct. 10, 1980).[2] FISA cannot infringe the President's inherent power under the Constitution to conduct national security searches, just as Congress cannot enact legislation that would interfere with the President's Commander-in-Chief power to conduct military hostilities. In either case, congressional efforts to regulate the exercise of an inherent executive power would violate the separation of powers by allowing the legislative branch to usurp the powers of the executive. *See* Memorandum for Timothy E. Flanigan, Deputy Counsel to the President, from John C. Yoo, Deputy Assistant Attorney General, *Re: The President's Constitutional Authority to Conduct Military Operations Against Terrorists and Nations Supporting Them* (Sept. 25, 2001) (War Powers Resolution cannot constitutionally define or regulate the President's Commander-in-Chief authority). Indeed, as we will see in Part IV, the Fourth Amendment's structure and Supreme Court case law demonstrate that the executive may engage in warrantless searches so long as the search is reasonable.

The federal courts have recognized the President's constitutional authority to conduct warrantless searches for national security purposes. To be sure, the Supreme Court has held that the warrant requirement should apply in cases of terrorism by purely domestic groups, *see United States v. United States District Court for the Eastern District of Michigan*, 407 U.S. 297, 299 (1972) ("*Keith*"), and has explicitly has not reached the scope of the President's surveillance powers with respect to the activities of foreign powers, *id.* at 308; *see also Katz. v. United States*, 389 U.S. 347, 358 n.23 (1967); *Mitchell*

---

[1]A short description of this history is attached to this letter.

[2]Based on similar reasoning, this Office has concluded that the President could receive materials, for national defense purposes, acquired through Title III surveillance methods or grand juries. Memorandum for Frances Fragos Townsend, Counsel, Office of Intelligence Policy and Review, from Randolph D. Moss, Assistant Attorney General, *Re: Title III Electronic Surveillance Material and the Intelligence Community* (Oct. 17, 2000); Memorandum for Gerald A. Schroeder, Acting Counsel, Office of Intelligence Policy and Review, from Richard L. Shiffrin, Deputy Assistant Attorney General, *Re: Grand Jury Material and the Intelligence Community* (Aug. 14, 1997); *Disclosure of Grand Jury Matters to the President and Other Officials*, 17 Op. O.L.C. 59 (1993).

v. Forsyth, 472 U.S. 511, 531 (1985). Nevertheless, even after *Keith* the lower courts have continued to find that when the government conducts a search for national security reasons, of a foreign power or its agents, it need not meet the same requirements that would normally apply in the context of criminal law enforcement, such as obtaining a judicial warrant pursuant to a showing of probable cause. *See, e.g., United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); *United States v. Buck*, 548 F.2d 871 (9th Cir.), *cert. denied* 434 U.S. 890 (1977); *United States v. Butenko*, 494 F.2d 593 (en banc), *cert. denied*, 419 U.S. 881 (1974); *United States v. Clay*, 430 F.2d 165 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971). Indeed, even FISA – which does not require a showing of probable cause – represents congressional agreement with the notion that surveillance conducted for national security purposes is not subject to the same Fourth Amendment standards that apply in domestic criminal cases.

Truong Dinh Hung exemplifies the considerations that have led the federal courts to recognize the President's constitutional authority to conduct warrantless national security searches. Unlike the domestic law enforcement context, the President's enhanced constitutional authority in national security and foreign affairs justifies a freer hand in conducting searches without ex ante judicial oversight. As the Fourth Circuit found, "the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would . . . 'unduly frustrate' the President in carrying out his foreign affairs responsibilities." *Truong Dinh Hung*, 629 F.2d at 913. A warrant requirement would be inappropriate, the court observed, because it would limit the executive branch's flexibility in foreign intelligence, delay responses to foreign intelligence threats, and create the chance for leaks. *Id.* Further, in the area of foreign intelligence, the executive branch is paramount in its expertise and knowledge, while the courts would have little competence in reviewing the government's need for the intelligence information. *Id.* at 913-14. In order to protect individual privacy interests, however, the court limited the national security exception to the warrant requirement to cases in which the object of the search is a foreign power, its agents, or collaborators, and when the surveillance is conducted primarily for foreign intelligence reasons. *Id.* at 915. The other lower courts to have considered this question similarly have limited the scope of warrantless national security searches to those circumstances.

Here, it seems clear that the current environment falls within the exception to the warrant requirement for national security searches. Foreign terrorists have succeeded in launching a direct attack on important military and civilian targets within the United States. The President may find that terrorists constitute an ongoing threat against the people of the United States and their national government, and he may find that protecting against this threat is a compelling government interest. The government would be conducting warrantless searches in order to discover information that will prevent future attacks on the United States and its citizens. This surveillance may provide information on the strength of terrorist groups, the timing and methods of their attack, and the target. The fact that the foreign terrorists have operated, and may continue to operate, within the domestic United States, does not clothe their operations in the constitutional protections that apply to domestic criminal investigations. See Memorandum for Alberto R.

Gonzalez, Counsel to the President and William J. Haynes, II, General Counsel, Department of Defense, from John C. Yoo, Deputy Assistant Attorney General and Robert J. Delahunty, Special Counsel, Re: *Authority for Use of Military Force to Combat Terrorist Activities Within the United States* (Oct. 23, 2001). While some information might prove useful to law enforcement, the purpose of the surveillance program remains that of protecting the national security. As we have advised in a separate memorandum, a secondary law enforcement use of information, which was originally gathered for national security purposes, does not suddenly render the search subject to the ordinary Fourth Amendment standards that govern domestic criminal investigations. *See* Memorandum for David S. Kris, Associate Deputy Attorney General, from John C. Yoo, Deputy Assistant Attorney General, *Re: Constitutionality of Amending Foreign Intelligence Surveillance Act to Change the "Purpose" Standard for Searches* (Sept. 25, 2001).

Due to the President's paramount constitutional authority in the field of national security, a subject which we will discuss in more detail below, reading FISA to prohibit the President from retaining the power to engage in warrantless national security searches would raise the most severe of constitutional conflicts. Generally, courts will construe statutes to avoid such constitutional problems, on the assumption that Congress does not wish to violate the Constitution, unless a statute clearly demands a different construction. *See, e.g., Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Construction Trades Council*, 485 U.S. 568, 575 (1988). Unless Congress signals a clear intention otherwise, a statute must be read to preserve the President's inherent constitutional power, so as to avoid any potential constitutional problems. *Cf. Public Citizen v. Department of Justice*, 491 U.S. 440, 466 (1989) (construing Federal Advisory Committee Act to avoid unconstitutional infringement on executive powers); *Association of American Physicians & Surgeons v. Clinton*, 997 F.2d 898, 906-11 (D.C. Cir. 1993) (same). Thus, unless Congress made a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless searches in the national security area – which it has not – then the statute must be construed to avoid such a reading. Even if FISA's liability provisions were thought to apply, we also believe that for a variety of reasons they could not be enforced against surveillance conducted on direct presidential order to defend the nation from attack. This issue can be discussed in more detail, if desired.

III.

Having established that the President has the authority to order the conduct of electronic surveillance without a warrant for national security purposes, we now examine the justification under the Fourth Amendment for the specific searches that might arise. The Fourth Amendment declares that "the right of the people to be secure in their persons, houses, papers, and effects, against *unreasonable* searches and seizures, shall not be violated." U.S. Const. amend IV. The Amendment also declares that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." *Id.* This Part will discuss the reasons why several elements of a possible surveillance program would not even trigger Fourth Amendment

scrutiny because they would not constitute a "search" for constitutional purposes.

A.

Aspects of surveillance that do not involve United States persons and that occur extraterritorially do not raise Fourth Amendment concerns. As the Supreme Court has found, the Fourth Amendment does not apply to military or intelligence operations conducted against aliens overseas. *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). In *Verdugo-Urquidez*, the Court found that the purpose of the Fourth Amendment "was to restrict searches and seizures which might be conducted by the United States in domestic matters. *Id.* at 266. As the Court concluded, the Fourth Amendment's design was "to protect the people of the United States against arbitrary action by their own government; it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens outside of the United States territory." *Id.* Indeed, the Court reversed a court of appeals' holding that the Fourth Amendment applied extraterritorially because of its concern that such a rule would interfere with the nation's military operations abroad:

> The rule adopted by the Court of Appeals would apply not only to law enforcement operations abroad, but also to other foreign policy operations which might result in "searches or seizures." The United States frequently employs Armed Forces outside this country – over 200 times in our history – for the protection of American citizens or national security . . . . Application of the Fourth Amendment to those circumstances could significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest. Were respondent to prevail, aliens with no attachment to this country might well bring actions for damages to remedy claimed violations of the Fourth Amendment in foreign countries or in international waters. . . . [T]he Court of Appeals' global view of [the Fourth Amendment's] applicability would plunge [the political branches] into a sea of uncertainty as to what might be reasonable in the way of searches and seizures conducted abroad.

Id. at 273-74 (citations omitted). Here, the Court made clear that aliens had no Fourth Amendment rights to challenge activity by the United States conducted abroad.

Thus, as applied, elements of a surveillance program would not even raise Fourth Amendment concerns, because much of the communications that the NSA would intercept would be those of non-U.S. persons abroad. [redacted] for example, which B1 B3 themselves do not terminate or originate in the United States and do not involve a U.S. person, do not involve a "search or seizure" under the Fourth Amendment. Further, any communications between terrorists that occur wholly abroad, and in which none of the terrorist participants are U.S. persons, also do not trigger Fourth Amendment scrutiny. An even narrower program, which would limit the interception

of communications involving terrorists to those that originate or terminate outside the United States, further narrows the likelihood that communications between U.S. persons within the United States will be intercepted.

B.

Second, intercepting certain communications that move internationally may not raise a Fourth Amendment issue because of what is known as the "border search exception." A surveillance program could direct the interception of all communications to or from another country in which terrorists are operating, which by definition would be international communication. Therefore, much if not all of the communications to be intercepted would cross the borders of the United States.

Under the border search exception to the Fourth Amendment, the federal government has the constitutional authority to search anything or anyone crossing the borders of the United States without violating any individual rights. In *United States v. Ramsey*, 431 U.S. 606 (1977), the Supreme Court upheld the constitutionality of searching incoming international mail based on reasonable cause to suspect that such mail contained illegally imported merchandise. Recognizing what it characterized as a "border search exception" to the Fourth Amendment's warrant and probable cause requirements, the Court observed that "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *Id.* at 616. The Court made clear that the manner in which something or someone crossed the border made no difference. "It is clear that there is nothing in the rationale behind the border search exception which suggests that the mode of entry will be critical." *Id.* at 620. The Court also observed that there was no distinction to be drawn in what crossed the border; "[i]t is their entry into this country from without it that makes a resulting search 'reasonable.'" *Id.* Although the Supreme Court has not examined the issue, the lower courts have unanimously found that the border search exception also applies to the exit search of outgoing traffic as well.[3]

Based on this doctrine, the interception of international communications could be justified by analogizing to the border search of international mail. Although electronic mail is, in some sense, intangible, it is also a message that begins at a physical server computer and then, though the movement of digital signals across wires, is transmitted to another server computer in a different location. Electronic mail is just

---

[3] *See, e.g., United States v. Oriakhi*, 57 F.3d 1290 (4th Cir. 1995); *United States v. Berisha*, 925 F.2d 791 (5th Cir. 1991); *United States v. Ezeiruaku*, 936 F.2d 136 (3d Cir. 1991); *United States v. Nates*, 831 F.2d 860 (9th Cir. 1987), *cert. denied*, 487 U.S. 1205 (1988); *United States v. Hernandez-Salazar*, 813 F.2d 1126 (11th Cir. 1987); *United States v. Benevento*, 836 F.2d 60 (2d Cir. 1987), *cert. denied*, 486 U.S. 1043 (1988); *United States v. Udofot*, 711 F.2d 831 (8th Cir.), *cert. denied*, 464 U.S. 896 (1983).

a different method of transporting a communication across the border of the United States. As the Court emphasized in *Ramsey*, "[t]he critical fact is that the envelopes cross the border and enter this country, not that they are brought in by one mode of transportation rather than another." *Id.* at 620. The fact that the method of transportation is electronic, rather than physical, should not make a difference, nor should it matter that the search does not occur precisely when the message crosses the nation's borders. Indeed, searches of outbound or inbound international mail or luggage take place at facilities within the nation's borders, after they have arrived by air, just as searches of electronic messages could occur once an international message appears on a server within the United States after transmission across our borders. It should be admitted that we have not found any cases applying *Ramsey* in this manner, although we also have not found any reported cases in which a court was confronted with a search effort of all international communications either.

There are three further caveats to raise in regard to the border search exception theory. First, it is altogether unclear whether *Ramsey* would apply at all to telephone conversations. While telephone conversations are like letters in that they convey messages, they are also ongoing, real-time transactions which do not contain discrete, self-contained chunks of communication. Second, and related to the first point, the Court has cautioned that examination of international mail for its content would raise serious constitutional questions. In *Ramsey*, the government opened outgoing mail that it suspected contained illegal drugs; regulations specifically forbade customs officials from reading any correspondence. Thus, the crime there was not the content of the communication itself, although the content could have been related to the transportation of the illegal substance. First Amendment issues would be raised if the very purpose of opening correspondence was to examine its content. *Id.* at 623-24. Third, the Court observed that serious constitutional problems in *Ramsey* were avoided due to a probable cause requirement. While this Office has advised that a reasonableness standard might still be constitutional if applied to international mail searches, we also acknowledged that our conclusion was not free from doubt. *See* Memorandum for Geoffrey R. Greiveldinger, Counsel for National Security Matters, Criminal Division, from Teresa Wynn Roseborough and Richard L. Shiffrin, Deputy Assistant Attorneys General, *Customs Service Proposal for Outbound Mail Search Authority, Amendment of Titles 31 U.S.C. § 5317(b) and 39 U.S.C. § 3623(d)* (Oct. 31, 1995). In light of these caveats, we can conclude that the border search exception would apply most squarely to the acquisition of communication addressing information, which for reasons we discuss below is not content, but might not reach the interception of the contents of telephone or other electronic communication.

C.

Third, the interception of electronic mail for its non-content information should not raise Fourth Amendment concerns. Capturing only the non-content addressing information of electronic communications may be analogized to a "pen register." A pen register is a device that records the numbers dialed from a telephone. In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court found that the

warrantless installation of a pen register for a defendant's home phone line did not violate the Fourth Amendment because use of a pen register was not a "search" within the meaning of the Amendment. Applying the test set out in *Katz v. United States*, 389 U.S. 347 (1967), the Court evaluated whether a person could claim a "legitimate expectation of privacy" in the phone numbers dialed. It found that a person could not have a legitimate expectation of privacy, because they should know that they numbers dialed are recorded by the phone company for legitimate business purposes, and that a reasonable person could not expect that the numerical information he voluntarily conveyed to the phone company would not be "exposed." *Id.* at 741-46. Because pen registers do not acquire the contents of communication, and because a person has no legitimate expectation of privacy in the numbers dialed, the Court concluded, use of a pen register does not constitute a search for Fourth Amendment purposes.

The Court's blessing of pen registers suggests that a surveillance program that sought only non-content information from electronic messages would be similarly constitutional. An interception program for electronic mail, for example, could capture only non-content information in regard to which a reasonable person might not have a legitimate expectation of privacy. E-mail addresses, like phone numbers, are voluntarily provided by the sender to the internet service provider (ISP) in order to allow the company to properly route the communication. A reasonable person could be expected to know that an ISP would record such message information for their own business purposes, just as telephone companies record phone numbers dialed. Furthermore, other information such as routing and server information is not even part of the content of a message written by the sender. Rather, such information is generated by the ISP itself, as part of its routine business operations, to help it send the electronic message through its network to the correct recipient. A sender could have no legitimate expectation of privacy over information he did not even include in his message, but instead is created by the ISP as part of its own business processes. A person would have no more privacy interest in that information than he would have in a postmark stamped onto the outside of an envelope containing his letter.

Whether a surveillance program involving electronic mail would sweep in content poses a more difficult question. From *Smith,* it appears that a pen register does not effectuate a Fourth Amendment search, in part, because it does not capture content from a communication. "Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed." *Smith*, 442 U.S. at 741. Here, it is no doubt true that electronic mail addressing information, created by the author of a communication, could contain some content. Variations of an addressee's name are commonly used to create e-mail addresses, and elements of the address can reveal other information, such as the institution or place someone works – hence, my e-mail address, assigned to me by the Justice Department, is john.c.yoo@usdoj.gov. This, however, does not render such information wholly subject to the Fourth Amendment. Even phone numbers can provide information that contains content. Phone numbers, for example, are sometimes used to spell words (such as 1-800-CALL-ATT), phone numbers can provide some location information, such as if someone calls a well-known hotel's number, and keypunches can even send messages, such as through pager systems. We believe that an individual's willingness to convey

to an ISP addressing information, which the ISP then uses for its own business purposes, suggests that an individual has no legitimate expectation of privacy in the limited content that could be inferred from e-mail addresses. We also note, however, that the courts have yet to encounter this issue in any meaningful manner, and so we cannot predict with certainty whether the judiciary would agree with our approach.

It should be noted that Congress has recognized the analogy between electronic mail routing information and pen registers. It recently enacted legislation authorizing pen register orders for non-content information from electronic mail. See USA Patriot Act of 2001, Pub. L. No. 107-56, § 216. While Congress extended pen register authority to surveillance of electronic mail, it also subjected that authority to the general restrictions of Title III and FISA, which require the Justice Department to obtain an ex parte court order before using such devices. While the requirements for such an order are minimal, see 18 U.S.C. § 3122 (government attorney must certify only that information likely to be gained from pen register "is relevant to an ongoing criminal investigation being conducted by that agency"), a warrantless surveillance program would not seek a judicial order for the surveillance program here. Title III attempts to forbid the use of pen registers or, now, electronic mail trap and trace devices, without a court under Title III or FISA. *Id.* at § 3121(a). As with our analysis of FISA, however, we do not believe that Congress may restrict the President's inherent constitutional powers, which allow him to gather intelligence necessary to defend the nation from direct attack. *See supra.* In any event, Congress's belief that a court order is necessary before using a pen register does not affect the constitutional analysis under the Fourth Amendment, which remains that an individual has no Fourth Amendment right in addressing information. Indeed, the fact that use of pen register and electronic trap and trace devices can be authorized without a showing of probable cause demonstrates that Congress agrees that such information is without constitutional protections.

D.

Fourth, intelligence gathering in direct support of military operations does not trigger constitutional rights against illegal searches and seizures. Our Office has recently undertaken a detailed examination of whether the use of the military domestically in order to combat terrorism would be restricted by the Fourth Amendment. *See* Memorandum for Alberto R. Gonzalez, Counsel to the President and William J. Haynes, II, General Counsel, Department of Defense, from John C. Yoo, Deputy Assistant Attorney General and Robert J. Delahunty, Special Counsel, Re: *Authority for Use of Military Force to Combat Terrorist Activities Within the United States* (Oct. 23, 2001). While we will only summarize here our reasoning, it should be clear that to the extent that a surveillance program is aimed at gathering intelligence for the military purpose of using the Armed Forces to prevent further attacks on the United States, that activity in our view is not restricted by the Fourth Amendment.

As a matter of the original understanding, the Fourth Amendment was aimed primarily at curbing law enforcement abuses. Although the Fourth Amendment has been interpreted to apply to governmental actions other than criminal law enforcement, the central concerns of the Amendment are focused on police

activity. *See, e.g., South Dakota v. Opperman*, 428 U.S. 364, 370 n.5 (1976). As we will explain in further detail in Part IV below, the Court has recognized this by identifying a "special needs" exception to the Fourth Amendment's warrant and probable cause requirements. *See, e.g., Vernonia School Dist. 47J v. Acton*, 515 U.S. 646 (1995); *Indianapolis v. Edmond*, 531 U.S. 32 (2000). However well suited the warrant and probable cause requirements may be as applied to criminal investigation and law enforcement, they are unsuited to the demands of wartime and the military necessity to successfully prosecute a war against an enemy. In the circumstances created by the September 11 attacks, the Constitution provides the Government with expanded powers and reduces the restrictions created by individual civil liberties. As the Supreme Court has held, for example, in wartime the government may summarily requisition property, seize enemy property, and "even the personal liberty of the citizen may be temporarily restrained as a measure of public safety." *Yakus v. United States*, 321 U.S. 414, 443 (1944) (citations omitted). "In times of war or insurrection, when society's interest is at its peak, the Government may detain individuals whom the Government believes to be dangerous." *United States v. Salerno*, 481 U.S. 739, 748 (1987); *see also Moyer v. Peabody*, 212 U.S. 78 (1909) (upholding detention without probable cause during time of insurrection) (Holmes, J.).

Because of the exigencies of war and military necessity, the Fourth Amendment should not be read as applying to military operations. In *Verdugo-Urquidez*, discussed in Part III, the Court made clear that the Fourth Amendment does not apply to military operations overseas. 494 U.S. at 273-274. As the Court observed, if things were otherwise, both political leaders and military commanders would be severely constrained by having to assess the "reasonableness" of any military action beforehand, thereby interfering with military effectiveness and the President's constitutional responsibilities as Commander-in-Chief. It also seems clear that the Fourth Amendment would not restrict military operations within the United States against an invasion or rebellion. *See, e.g.*, 24 Op. Att'y Gen. 570 (1903) (American territory held by enemy forces is considered hostile territory where civil laws do not apply). Were the United States homeland invaded by foreign military forces, our armed forces would have to take whatever steps necessary to repel them, which would include the "seizure" of enemy personnel and the "search" of enemy papers and messages, it is difficult to believe that our government would need to show that these actions were "reasonable" under the Fourth Amendment. The actions of our military, which might cause collateral damage to United States persons, would no more be constrained by the Fourth Amendment than if their operations occurred overseas. Nor is it necessary that the military forces on our soil be foreign. Even if the enemies of the Nation came from within, such as occurred during the Civil War, the federal Armed Forces must be free to use force to respond to such an insurrection or rebellion without the constraints of the Fourth Amendment. Indeed, this was the understanding that prevailed during the Civil War.

These considerations could justify much of a warrantless electronic surveillance program. Although the terrorists who staged the September 11, 2001 events operated clandestinely and have not occupied part of our territory, they have launched a direct attack on both the American homeland and our assets overseas that have caused massive casualties. Their attacks were launched and carried out from within the

United States itself. Pursuant to his authority as Commander-in-Chief and Chief Executive, the President has ordered the use of military force against the terrorists both at home and abroad, and he has found that they present a continuing threat of further attacks on the United States. Application of the Fourth Amendment could, in many cases, prevent the President from fulfilling his highest constitutional duty of protecting and preserving the Nation from direct attack. Indeed, the opposite rule would create the bizarre situation in which the President would encounter less constitutional freedom in using the military when the Nation is directly attacked at home, where the greatest threat to American civilian casualties lies, than we use force abroad.

Thus, the Fourth Amendment should not limit military operations to prevent attacks that take place within the American homeland, just as it would not limit the President's power to respond to attacks launched abroad. A surveillance program, undertaken for national security purposes, would be a necessary element in the effective exercise of the President's authority to prosecute the current war successfully. Intelligence gathered through surveillance allows the Commander-in-Chief to determine how best to position and deploy the Armed Forces. It seems clear that the primary purpose of the surveillance program is to defend the national security, rather than for law enforcement purposes, which might trigger Fourth Amendment concerns. In this respect, it is significant that the President would be ordering the Secretary of Defense (who supervises the NSA), rather than the Justice Department, to conduct the surveillance, and that evidence would not be preserved for later use in criminal investigations. While such secondary use of such information for law enforcement does not undermine the primary national security purpose motivating the surveillance program, it is also clear that such intelligence material, once developed, can be made available to the Justice Department for domestic use.

IV.

Even if a surveillance program, or elements of it, were still thought to be subject to Fourth Amendment scrutiny, we think that compelling arguments can justify its constitutionality. This Part will review whether warrantless electronic surveillance, undertaken for national security purposes, is constitutional under the Fourth Amendment. It should be clear at the outset that the Fourth Amendment does not require a warrant for every search, but rather that a search be "reasonable" to be constitutional. In light of the current security environment, the government can claim a compelling interest in protecting the nation from attack sufficient to outweigh any intrusion into privacy interests.

A.

The touchstone for review of a government search is whether it is "reasonable." According to the Supreme Court, "[a]s the text of the Fourth Amendment indicates the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 652 (1995). When law enforcement undertakes a search to discover evidence of criminal

wrongdoing, the Supreme Court has said that reasonableness generally requires a judicial warrant on a showing of probable cause that a crime has been or is being committed. *Id.* at 653. But the Court has also recognized that a warrant is not required for all government searches, especially those that fall outside the ordinary criminal investigation context. A warrantless search can be constitutional "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Id.*

A variety of government searches, therefore, have met the Fourth Amendment's requirement of reasonableness without obtaining a judicial warrant. The Supreme Court, for example, has upheld warrantless searches that involved the drug testing of high school athletes, *id.*, certain searches of automobiles, *Pennsylvania v. Labron*, 518 U.S. 938 (1996) (per curiam), drunk driver checkpoints, *Michigan v. Dep't of State Police v. Sitz*, 496 U.S. 444 (1990), drug testing of railroad personnel, *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602 (1989), drug testing of federal customs officers, *Treasury Employees v. Von Raab*, 489 U.S. 656 (1989), administrative inspection of closely regulated businesses, *New York v. Burger*, 482 U.S. 691 (1987); temporary baggage seizures, *United States v. Place*, 462 U.S. 696 (1983), detention to prevent flight and to protect law enforcement officers, *Michigan v. Summers*, 452 U.S. 692 (1981), checkpoints to search for illegal aliens, *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976), and temporary stops and limited searches for weapons, *Terry v. Ohio*, 392 U.S. 1 (1968). The Court has cautioned, however, that a random search program cannot be designed to promote a general interest in crime control. *See Indianapolis v. Edmond*, 531 U.S. 32, 41 (2000); *Delaware v. Prouse*, 440 U.S. 648, 659 n.18 (1979).

Reasonableness does not lend itself to precise tests or formulations. Nonetheless, in reviewing warrantless search programs, the Court generally has balanced the government's interest against intrusion into privacy interests. "When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable." *Illinois v. McArthur*, 121 S. Ct. 946, 949 (2001). Or, as the Court has described it, warrantless searches may be justified if the government has "special needs" that are unrelated to normal law enforcement. In these situations, the Court has found a search reasonable when, under the totality of the circumstances, the "importance of the governmental interests" has outweighed the "nature and quality of the intrusion on the individual's Fourth Amendment interests." *Tennessee v. Garner*, 471 U.S. 1, 8 (1985).

B.

This analysis suggests that the Fourth Amendment would permit warrantless electronic surveillance if the government's interest outweighs intrusions into privacy interests. It should be clear that the President's directive falls within the "special needs" exception to the warrant requirement that calls for such a balancing test. The surveillance program is not designed to advance a "general interest in crime control,"

Edmond, 531 U.S. at 44, but instead seeks to protect the national security by preventing terrorist attacks upon the United States. As the national security search cases discussed in Part II recognize, defending the nation from foreign threats is a wholly different enterprise than ordinary crime control, and this difference justifies examination of the government's action solely for its reasonableness. Indeed, as the Supreme Court recognized in *Edmond*, warrantless, random searches undertaken for national security purposes, such as forestalling a terrorist attack on an American city, would be constitutional even if the same search technique, when undertaken for general crime control, would fail Fourth Amendment standards.

Applying this standard, we find that the government's interest here is perhaps of the highest order --that of protecting the nation from attack. Indeed, the factors justifying warrantless searches for national security reasons are more compelling now than at the time of the earlier lower court decisions discussed in Part II. While upholding warrantless searches for national security purposes, those earlier decisions had not taken place during a time of actual hostilities prompted by a surprise, direct attack upon civilian and military targets within the United States. A direct attack on the United States has placed the Nation in a state of armed conflict; defending the nation is perhaps the most important function of government. As the Supreme Court has observed, "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981). As Alexander Hamilton observed in *The Federalist*, "there can be no limitation of that authority, which is to provide for the defence and protection of the community, in any matter essential to its efficacy." *The Federalist* No. 23, at 147-48 (Alexander Hamilton) (Jacob E. Cooke ed., 1961). If the situation warrants, the Constitution recognizes that the federal government, and indeed the President, must have the maximum power permissible under the Constitution to prevent and defeat attacks upon the Nation.

In authorizing an electronic surveillance program, the President should lay out the proper factual predicates for finding that the terrorist attacks had created a compelling governmental interest. The September 11, 2001 attacks caused thousands of deaths and even more casualties, and damaged both the central command and control facility for the Nation's military establishment and the center of the country's private financial system. In light of information that would be provided by the intelligence community and the military, the President could further conclude that terrorists continue to have the ability and the intention to undertake further attacks on the United States. Given the damage caused by the attacks on September 11, 2001, the President could judge that future terrorist attacks could cause massive damage and casualties and threatens the continuity of the federal government. He could conclude that such circumstances justify a compelling interest on the part of the government to protect the United States and its citizens from further terrorist attack. It seems certain that the federal courts would defer to the President's determination on whether the United States is threatened by attack and what measures are necessary to respond. *See, e.g., The Prize Cases*, 67 U.S. 635, 670 (1862) (decision whether to consider rebellion a war is a question to be decided by the President). These determinations rest at the core of the President's power as Commander-in-Chief and his role as representative of the Nation in its foreign affairs. *See United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304 (1936).

Under the Constitution's design, it is the President who is primarily responsible for advancing that compelling interest. The text, structure, and history of the Constitution establish that the President bears the constitutional duty, and therefore the power, to ensure the security of the United States in situations of grave and unforeseen emergency. *See generally* Memorandum for Timothy E. Flanigan, Deputy Counsel to the President, from John C. Yoo, Deputy Assistant Attorney General, *Re: The President's Constitutional Authority to Conduct Military Operations Against Terrorists and Nations Supporting Them* (Sept. 25, 2001). Both the Vesting Clause, U.S. Const. art. II, § 1, cl. 1, and the Commander in Chief Clause, *id.*, § 2, cl. 1, vest in the President the power to deploy military force in the defense of the United States. The Constitution makes explicit the President's obligation to safeguard the nation's security by whatever lawful means are available by imposing on him the duty to "take Care that the Laws be faithfully executed." *Id.*, § 3. The constitutional text and structure are confirmed by the practical consideration that national security decisions require a unity in purpose and energy in action that characterize the Presidency rather than Congress. As Alexander Hamilton explained, "[o]f all the cares or concerns of government, the direction of war most peculiarly demands those qualities which distinguish the exercise of power by a single hand." *The Federalist* No. 74, at 500 (Alexander Hamilton) (Jacob E. Cooke ed. 1961).

Surveillance initiated in response to the September 11 attacks would clearly advance this interest. The President would be exercising his powers as Commander-in-Chief and Chief Executive to direct military action against Al Qaeda and Taliban forces in Afghanistan, and to use the armed forces to protect United States citizens at home. Congress has approved the use of military force in response to the September 11 attacks. Pub. L. No. 107-40, 115 Stat. 224 (2001). It is well established that the President has the independent constitutional authority as Commander-in-Chief to gather intelligence in support of military and national security operations, and to employ covert means, if necessary, to do so. *See Totten v. United States*, 92 U.S. 105, 106 (1876). The President's "constitutional power to gather foreign intelligence," *Warrantless Foreign Intelligence Surveillance – Use of Television – Beepers*, 2 Op. O.L.C. 14, 15 (1978), includes the discretion to use the most effective means of obtaining information, and to safeguard those means. Intelligence gathering is a necessary function that enables the President to carry out these authorities effectively. The Commander-in-Chief needs accurate and comprehensive intelligence on enemy movements, plans, and threats in order to best deploy the United States armed forces and to successfully execute military plans. Warrantless searches could provide the most effective method, in the President's judgment, to obtain information necessary for him to carry out his constitutional responsibility to defend the Nation from attack.

By contrast, the intrusion into an individual citizen's privacy interests may not be seen as so serious as outweighing the government's most compelling of interests. The searches that would take place are as not as intrusive as those which occur when the government monitors the communications of a target in the normal Title III or FISA context. These often require an agent to consciously and actively listen in to telephone conversations. Here, as we understand it, [redacted] B1 B3

B1
B3

[redacted]

If privacy interests are viewed as intruded upon only by [redacted] it is likely that Fourth Amendment interests would not outweigh the compelling governmental interest present here. In the context of roadblocks to stop drunken drivers, another area of "special needs" under the Fourth Amendment, the Court has permitted warrantless searches. *See Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990). There, the Court found that a roadblock constituted a "reasonable" search due to the magnitude of the drunken driver problem and the deaths it causes – in fact, the court compared the death toll from drunk drivers to the casualties on a battlefield. *Id.* at 451. It found that this interest outweighed the intrusion into privacy at a checkpoint stop, which it characterized as "brief" in terms of duration and intensity. Similarly, [redacted] than in the case of a roadblock, where a [redacted] law enforcement officer stops each driver to examine whether they are inebriated. It seems that if the Supreme Court were willing to uphold drunk driver checkpoints, it would be equally or even more willing to allow [redacted][4]

B1
B3

B1
B3

B1
B3

The restriction of a surveillance program only to those communications which originate or terminate in a foreign country or which involve terrorists further reduces any possible intrusion into individual privacy interests. If probable cause is required, it seems that DOD would need specific evidence before deciding which messages to intercept. Thus, for example, DOD must have some information that a certain person might be a terrorist, or that a certain phone line might be used by a terrorist, before it can capture the communications. This means that the NSA cannot intercept communications for which it has no such evidence. This would be the case even if the President were to require that there be reasonable grounds to believe that the communications involve the relevant foreign country or terrorists. This has the effect of excluding communications for which DOD has no reason to suspect contain terrorist communications or communications with the foreign country, meaning that most innocent communications will not be

---

[4]Another factor examined by the Court was effectiveness of the warrantless search. The Court has cautioned that searches not be random and discretionless because of a lack of empirical evidence that the means would promote the government's interest. It should be made clear, however, that the standard employed by the Court has been low. In the roadblock context, for example, the Court has found reasonable roadblocks for drunk drivers that detained only 1.6 percent of all drivers stopped, and checkpoints for illegal aliens that detained only 0.12 percent of all vehicles detained.

intercepted.

Further, limiting the search parameters to international communications could further alleviate any intrusion into individual privacy interests. As our discussion of the border search exception in Part III made clear, the government has the constitutional authority to search anything that crosses the Nation's borders without violating the Fourth Amendment. To be sure, there is substantial doubt about whether this power could apply to searches involving the content of the communications. Nonetheless, *United States v. Ramsey*, 431 U.S. 606 (1977) (warrantless search of incoming international mail does not violate Fourth Amendment), suggests strongly that individuals have reduced privacy interests when they or their possessions and letters cross the borders of the United States. If individuals have reduced privacy interests in international mail, as *Ramsey* held, then it seems logical to assume that they also have a reduced privacy interest in international electronic communications as well. As *Ramsey* held, the method by which an item entered the country is irrelevant for Fourth Amendment purposes.

Just to be clear in conclusion. We are not claiming that the government has an unrestricted right to examine the contents of all international letters and other forms of communication. Rather, we are only suggesting that an individual has a reduced privacy interest in international communications Therefore, in applying the balancing test called for by the Fourth Amendment's reasonableness analysis, we face a situation here where the government's interest on one side – that of protecting the Nation from direct attack – is the highest known to the Constitution. On the other side of the scale, the intrusion into individual privacy interests is greatly reduced due to the international nature of the communications. Thus, we believe there to be substantial justification for a warrantless electronic surveillance program, undertaken in response to the September 11, 2001 attacks, that would be reasonable under the Fourth Amendment.

I would welcome the opportunity to discuss these issues in more detail. Please contact me, at 202-514-2069, or john.c.yoo@usdoj.gov, if you have any further questions.

Sincerely,

John Yoo

John C. Yoo
Deputy Assistant Attorney General

AUTHORITY FOR WARRANTLESS NATIONAL SECURITY SEARCHES

Presidents have long asserted the constitutional authority to order searches, even without judicial warrants, where necessary to protect the national security against foreign powers and their agents. The courts have repeatedly upheld the exercise of this authority.

A memorandum from President Franklin D. Roosevelt to Attorney General Robert H. Jackson, dated May 21, 1940, authorized the use of wiretaps in matters "involving the defense of the nation." *See United States v. United States District Court for the Eastern District of Michigan*, 407 U.S. 297, 311 n.10 (1972) ("*Keith*"). The President directed the Attorney General "to secure information by listening devices [directed at] the conversation or other communications of persons suspected of subversive activities against the government of the United States, including suspected spies," while asking the Attorney General "to limit these investigations so conducted to a minimum and to limit them insofar as possible as to aliens." *See* Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearings Before the Subcomm. on Intelligence and the Rights of Americans of the Select Comm. on Intelligence, 94th Cong., 2d Sess. 24 (1976) (statement of Attorney General Edward H. Levi) ("Levi Statement"). President Roosevelt issued the memorandum after the House of Representatives passed a joint resolution to sanction wiretapping by the FBI for national security purposes, but the Senate failed to act. *See* Americo R. Cinquegrana, *The Walls and Wires Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. Pa. L. Rev. 793, 797-98 (1989).

By a letter dated July 17, 1946, Attorney General Tom C. Clark reminded President Truman of the 1940 directive, which had been followed by Attorneys General Jackson and Francis Biddle. At Attorney General Clark's request, the President approved the continuation of the authority, *see* Levi Statement at 24, and even broadened it to reach "internal security cases." *Keith*, 407 U.S. at 311 and n.10. In the Eisenhower Administration, Attorney General Herbert Brownell, as the Supreme Court noted in *Keith*, advocated the use electronic surveillance both in internal and international security matters. 407 U.S. at 311.

In 1965, President Johnson announced a policy under which warrantless wiretaps would be limited to national security matters. Levi Statement at 26. Attorney General Katzenbach then wrote that he saw "no need to curtail any such activities in the national security field." *Id.* Attorney General Richardson stated in 1973 that, to approve a warrantless surveillance, he would need to be convinced that it was necessary "(1) to protect the nation against actual or potential attack or other hostile acts of a foreign power, (2) to obtain foreign intelligence information deemed essential to the security of the United States, or (3) to protect national security information against foreign intelligence activities." *Id.* at 27. When Attorney General Levi testified in 1976, he gave a similar list, adding that a warrantless surveillance could also be used "to obtain information certified as necessary for the conduct of foreign

affairs matters important to the national security of the United States." *Id.*

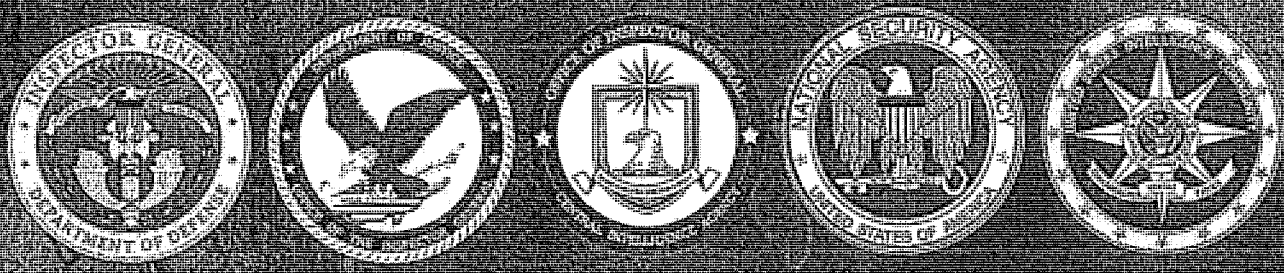
Warrantless electronic surveillance of agents of foreign powers thus continued until the passage in 1978 of the Foreign Intelligence Surveillance Act, 18 U.S.C. §§ 1801-29. Although the Supreme Court never ruled on the legality of warrantless searches as to agents of foreign powers, *see Keith*, 407 U.S. at 321-22 (requiring a warrant in domestic security cases but reserving issue where a foreign power or its agents were involved), the courts of appeals repeatedly sustained the lawfulness of such searches. *United States v. Truong Dinh Hung*, 629 F.2d 908, 914 (4th Cir. 1980); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973); *United States v. Butenko*, 494 F.2d 593, 606 (3d Cir. 1974); *United States v. Clay*, 430 F.2d 165 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971); *but see Zweibon v. Mitchell*, 516 F.2d 594, 651 (D.C. Cir. 1975) (dictum in plurality opinion). The Fourth Circuit held, for example, that "because of the need of the executive branch for flexibility, its practical experience, and its constitutional competence, the courts should not require the executive to secure a warrant each time it conducts foreign intelligence surveillance." *Truong*, 629 F.2d at 914. As the court elaborated, "attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy," and a "warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations." *Id.* at 913 (citations and footnote omitted). Furthermore, "the executive possesses unparalleled expertise to make the decisions whether to conduct foreign intelligence surveillance." *Id.* (citations omitted). And "[p]erhaps most crucially, the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs." *Id.* at 914 (citations omitted). In this pre-statutory context, two courts of appeals, the Fourth Circuit in *Truong* (*id.* at 915) and the Third Circuit in *Butenko* (494 F.2d at 606), would have limited the authority to instances where the primary purpose of the search was to obtain foreign intelligence."

The passage of FISA created an effective means for issuance of judicial orders for electronic surveillance in national security matters. Congress, however, had not given the Foreign Intelligence Surveillance Court the power to issue orders for physical searches. After nevertheless granting orders in three instances during the Carter Administration, the court ruled early in the Reagan Administration, as the Justice Department then argued, that it lacked jurisdiction to approve physical searches. *See* S. Rep. 103-296, at 36-37 (1994). Thus, physical searches after the ruling had to approved by the Attorney General without a judicial warrant. *Id.* at 37. In 1994, after the use of warrantless physical searches in the Aldrich Ames case, Congress concluded that "from the standpoint of protecting the constitutional rights of Americans, from the standpoint of bringing greater legal certainty to this area, from the standpoint of avoiding problems with future espionage prosecutions, and from the standpoint of protecting federal officers and employees from potential civil liability," *id.*, FISA should be amended to cover physical searches. *Id.* at 40.

(U) REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

VOLUME I

10 JULY 2009



PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Special Warning

The report contains compartmented, classified material and no secondary distribution may be made without prior consent of the participating Inspectors General. Improper disclosure of this report may result in criminal, civil, or administrative penalties.

REPORT NO. 2009-0013-AS

10 July 2009

(U) Preface

(U) Title III of the Foreign Intelligence Surveillance Act Amendments Act of 2008 required the Inspectors General (IGs) of the elements of the Intelligence Community that participated in the President's Surveillance Program (PSP) to conduct a comprehensive review of the Program. The IGs of the Department of Justice (DoJ), the Department of Defense (DoD), the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Office of the Director of National Intelligence (ODNI) participated in the review required under the Act. The Act required the IGs to submit a comprehensive report on the review to the Senate Select Committee on Intelligence, the Senate Committee on the Judiciary, the House Permanent Select Committee on Intelligence, and the House Committee on the Judiciary.

(U) Because many aspects of the PSP remain classified, and in order to provide the Congressional committees the complete results of our review, we have prepared this classified report on the PSP. The report is in three volumes:

- Volume I summarizes the collective results of the IGs' review.
- Volume II contains the individual reports prepared and issued by the DoD, CIA, NSA, and ODNI IGs.
- Volume III contains the report prepared and issued by the DoJ IG.

(U) The unclassified report on the PSP required by Title III has been provided to the Congressional committees in a separately bound volume.

Unclassified When Separated
From Attachment

~~Derived From: NSA/CSSM 1-52, 2-400,~~
~~NSA/CSS M 1-52, 12-48~~
~~Dated: 20070108~~
~~Declassify On: 20340713~~

Glenn A. Fine
Inspector General
Department of Justice

Gordon S. Heddell
Acting Inspector General
Department of Defense

Patricia A. Lewis
Acting Inspector General
Central Intelligence Agency

George Ellard
Inspector General
National Security Agency

Roslyn A. Mazer
Inspector General
Office of the Director of
National Intelligence

(U) Table of Contents

(U) INTRODUCTION 1

(U) Scope of the Review 1

(U) Methodology 2

(U) INCEPTION OF THE PRESIDENT'S SURVEILLANCE PROGRAM 4

(U) National Security Agency Counterterrorism Efforts Prior to 11 September 2001 4

(U) NSA Initially Used Existing Authorities to Enhance Signals Intelligence (SIGINT) Collection After the September 2001 Terrorist Attacks 5

(U) NSA Explored Options to Improve SIGINT Collection and Address Intelligence Gaps on Terrorist Targets 6

(U) Impediments to SIGINT Collection Against Terrorist Targets Were Discussed With the White House 7

(U) Authorization of the President's Surveillance Program 7

(U) SIGINT Activities Authorized Under the Program 7

(U) Content of the Presidential Authorizations and Department of Justice Certification as to Form and Legality 9

(U) The Threat Assessment Memorandums Supporting Presidential Authorization of the Program 10

(U) Early Revisions to the Presidential Authorizations 11

(U) DoJ Office of Legal Counsel Memorandums Supporting Legality of the Program 12

(U) IMPLEMENTATION OF THE PRESIDENT'S SURVEILLANCE PROGRAM 16

(U) NSA Implementation 16

[redacted] 17

~~(TS//SI//NF)~~ Telephone and Internet Communications Content Collection and Analysis 18

~~(TS//SI//NF)~~ Telephony and Internet Metadata Collection and Analysis 20

(U) NSA Reporting From the President's Surveillance Program 21

(U) NSA Managerial Structure and Oversight of the President's Surveillance Program 22

(U) NSA Management Controls to Ensure Compliance With Presidential Authorizations 23

(U) NSA Inspector General Oversight of the Program 24

(U) Access to the President's Surveillance Program 25

(U) Congressional Briefings on the Program 26

(U) Foreign Intelligence Surveillance Court Briefings on the Program 27

(U) FBI Participation in the President's Surveillance Program 28

(U) CIA Participation in the President's Surveillance Program 30

(U) NCTC Participation in the President's Surveillance Program 32

(U) The President's Surveillance Program and the Foreign Intelligence Surveillance Court 33

(U) Discovery Issues Associated With the President's Surveillance Program 35

(U) LEGAL REASSESSMENT OF THE PRESIDENT'S SURVEILLANCE PROGRAM (2003 – 2004) 36

~~(TS//SI//NF)~~ Concern Over the [redacted] Collection 36

(U) A New Legal Basis for the Program Is Adopted 37

(U) Department of Justice Officials Convey Concerns About the Program to the White House 39

(U) Conflict Between the Department of Justice and the White House Over the Program 40

~~(S//NF)~~ White House Counsel Certifies Presidential Authorization Without Department of Justice Concurrence 44

~~(TS//SI//NF)~~ White House Agrees to [redacted] 48

(U) Restrictions on Access to the President's Surveillance Program Impeded Department of Justice Legal Review 50

(U) TRANSITION OF PRESIDENT'S SURVEILLANCE PROGRAM ACTIVITIES TO FOREIGN INTELLIGENCE SURVEILLANCE ACT AUTHORITY 50

~~(TS//SI//NF)~~ Internet Metadata Collection Transition to Operation Under FISA Authority 50

(U) Department of Justice Notices of Compliance Incidents 53

~~(TS//SI//NF)~~ Telephony Metadata Collection Transition to Operation Under FISA Authority 54

~~(TS//SI//NF)~~ Content Collection Transition to Operation Under FISA Authority 57

(U) IMPACT OF THE PRESIDENT'S SURVEILLANCE PROGRAM ON INTELLIGENCE COMMUNITY COUNTERTERRORISM EFFORTS 60

(U) Senior Intelligence Community Officials Believe That the President's Surveillance Program Filled an Intelligence Gap 60

(U) Difficulty in Assessing the Impact of the President's Surveillance Program 61

(U) Impact of the President's Surveillance Program on FBI Counterterrorism Efforts 61

(U) FBI Efforts to Assess the Value of the Program 62

(U) FBI Judgmental Assessments of the Program 62

(U) Impact of the President's Surveillance Program on CIA Counterterrorism Operations 63

(U) The CIA Did Not Systematically Assess the Effectiveness of the Program 63

(U) Several Factors Hindered CIA Utilization of the Program 64

(U) Impact of the President's Surveillance Program on NCTC Counterterrorism Efforts 65

(U) Counterterrorism Operations Supported by the President's Surveillance Program 65

(U) ATTORNEY GENERAL GONZALES'S TESTIMONY ON THE PRESIDENT'S SURVEILLANCE PROGRAM 68

(U) CONCLUSIONS 69

(U) The President's Surveillance Program

(U) INTRODUCTION

~~(TS//SI//OC/NF)~~ In response to the terrorist attacks of 11 September 2001, on 4 October 2001, President George W. Bush issued a Top Secret authorization to the Secretary of Defense directing that the signals intelligence (SIGINT) capabilities of the National Security Agency (NSA) be used to detect and prevent further attacks in the United States. The Presidential Authorization stated that an extraordinary emergency existed permitting the use of electronic surveillance within the United States for counterterrorism purposes, without a court order, under certain circumstances. For more than five years, the Presidential Authorization was renewed at 30- to 60-day intervals to authorize the highly classified NSA surveillance program, which is referred to throughout this report as the President's Surveillance Program (PSP).[1]

~~(TS//SI//OC/NF)~~ Under the Presidential Authorizations, the NSA intercepted the content of international telephone and Internet communications of both U.S. and non-U.S. persons. In addition, the NSA collected telephone and Internet metadata—communications signaling information showing contacts between and among telephone numbers and Internet communications addresses, but not including the contents of the communications. [redacted] The content and metadata information was analyzed by the NSA, working with other members of the Intelligence Community (IC), to generate intelligence reports. These reports were sent to the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and other intelligence organizations.

(U) The scope of collection permitted under the Presidential Authorizations varied over time. In stages between July 2004 and January 2007, NSA ceased PSP collection activities under Presidential authorization and resumed them under four separate court orders issued in accordance with the Foreign Intelligence Surveillance Act of 1978 as amended (FISA).[2]

(U) Scope of the Review

(U) Title III of the Foreign Intelligence Surveillance Act Amendments Act of 2008 (FISA Amendments Act)—signed into law on 10 July 2008—required the inspectors

---

[1] ~~(S//NF)~~ The cover term NSA uses to protect the President's Surveillance Program is STELLARWIND.

[2] (U) Unless otherwise indicated, references to FISA in this report are to the statute as it existed prior to being amended in 2008.

general of the elements of the IC that participated in the PSP to conduct a comprehensive review of the program.[3] The Act required that the review examine:

> (A) all of the facts necessary to describe the establishment, implementation, product, and use of the product of the Program;
>
> (B) access to legal reviews of the Program and access to information about the Program;
>
> (C) communications with, and participation of, individuals and entities in the private sector related to the Program;
>
> (D) interaction with the Foreign Intelligence Surveillance Court and transition to court orders related to the Program; and
>
> (E) any other matters identified by any such Inspector General that would enable that Inspector General to complete a review of the Program, with respect to such Department or element.

(U) The Inspectors General (IGs) of the Department of Defense (DoD), the Department of Justice (DoJ), the CIA, the NSA, and the Office of the Director of National Intelligence (ODNI) conducted the review required under the Act. This report summarizes the collective results of the IGs' review. Conclusions and recommendations in this report that are attributed to a particular IG should be understood to represent that IG's opinion. Individual reports detail the results of each IG's review and are annexes to this report. All of the reports have been classified in accordance with the program's classification guide, which was revised during our review and re-issued on 21 January 2009.

(U) Title III of the FISA Amendments Act also required that the report of any investigation of matters relating to the PSP conducted by the DoJ, Office of Professional Responsibility (OPR) be provided to the DoJ IG, and that the findings and conclusions of such investigation be included in the DoJ IG's review. OPR intends to review whether any standards of professional conduct were violated in the preparation of the first series of legal memorandums supporting the PSP. OPR has not yet completed its review or provided its findings and conclusions to the DoJ IG.

(U) Methodology

(U) During the course of this review, the participating IGs conducted approximately 200 interviews. Among the individuals we interviewed were: former White House Counsel and Attorney General Alberto R. Gonzales; former Deputy Attorney General James B. Comey; FBI Director Robert S. Mueller, III; former Secretary of Defense

---

[3] (U) The President's Surveillance Program is defined in the Act as the intelligence activity involving communications that was authorized by the President during the period beginning on 11 September 2001 and ending on 17 January 2007, including the program referred to by the President in a radio address on 17 December 2005 (commonly known as the Terrorist Surveillance Program).

Donald H. Rumsfeld; former NSA Director, Principal Deputy Director of National Intelligence, and CIA Director Michael V. Hayden; former Director of Central Intelligence (DCI) and CIA Director Porter J. Goss; NSA Director Lieutenant General Keith B. Alexander; former Directors of National Intelligence John D. Negroponte and J. M. McConnell; and former National Counterterrorism Center (NCTC) Director John O. Brennan. Certain other persons who had significant involvement in the PSP either declined or did not respond to our requests for an interview, including former Deputy Secretary of Defense Paul D. Wolfowitz; former Chief of Staff to President Bush Andrew H. Card; David S. Addington, former Counsel to Vice President Richard B. Cheney; former Attorney General John D. Ashcroft; former Deputy Assistant Attorney General John Yoo; and former DCI George J. Tenet.

~~(S//NF)~~ We interviewed former NSA [redacted] as well as leadership [redacted] within the NSA Signals Intelligence Directorate (SID). We interviewed personnel from the CIA [redacted]; senior FBI Counterterrorism Division officials; FBI special agents and intelligence analysts; senior officials from DoJ's Criminal and National Security Divisions; and current and former senior NCTC officials. We also interviewed DoJ officials and office of general counsel officials from the participating organizations who were involved in legal reviews of the PSP and/or had access to the memorandums supporting the legality of the PSP.

~~(S//NF)~~ We examined thousands of electronic and hardcopy documents, including the Presidential Authorizations, terrorist threat assessments, legal memorandums, applicable regulations and policies, briefings, reports, correspondence, and notes. We obtained access to an FBI database of PSP-derived leads that had been disseminated to FBI field offices. We used the database to confirm information obtained through interviews and to assist in our analysis of FBI investigations that utilized PSP information. We evaluated the justifications included in the requests for information (RFIs) submitted by the CIA to the NSA to determine whether they were in accordance with program guidelines. Reports of prior reviews and investigations of the PSP conducted by the NSA IG were also utilized in our review.

(b)(1), (b)(3), (b)(7)(E)

[redacted]

b1,
b3,
b7E

(U) INCEPTION OF THE PRESIDENT'S SURVEILLANCE PROGRAM

(U) National Security Agency Counterterrorism Efforts Prior to 11 September 2001

~~(C//NF)~~ For more than a decade before the terrorist attacks of 11 September 2001, NSA was applying its SIGINT capabilities against terrorist targets in response to IC requirements.[3] The NSA, SID, Counterterrorism (CT) Product Line led these efforts. NSA was authorized by Executive Order (E.O.) 12333, *United States Intelligence Activities*, 4 December 1981, as amended, to collect, process, and disseminate SIGINT information for foreign intelligence and counterintelligence purposes in accordance with DCI guidance and to support the conduct of military operations under the guidance of the Secretary of Defense. It is the policy of U.S. Government entities that conduct SIGINT activities that they will collect, retain, and disseminate only foreign communications. In September 2001, NSA's compliance procedures defined foreign communications as communications having at least one communicant outside the United States, communications entirely among foreign powers, or communications between a foreign power and officers or employees of a foreign power. All other communications were considered domestic communications. NSA was not authorized under E.O. 12333 to collect communications from a wire in the United States without a court order unless the communications originated and terminated outside the United States or met applicable exceptions to the requirement of a court order under FISA.

(U) FISA, 50 U.S.C. § 1801, et seq., was enacted in 1978 to "provide legislative authorization and regulation for all electronic surveillance conducted within the United States for foreign intelligence purposes." FISA authorizes the Federal Government to engage in electronic surveillance and physical searches, to use pen register and trap and trace devices, and to obtain business records to acquire foreign intelligence information by targeting foreign powers and agents of foreign powers inside the United States.[4] As a general rule, the FISC must first approve an application for a warrant before the government may initiate electronic surveillance.

~~(S//SI//NF)~~ Prior to the PSP, NSA authority to intercept foreign communications included the Director, NSA's authority to approve the targeting of communications with one communicant within the United States if technical devices could be employed to limit collection to communications where the target is a non-U.S. person located outside the United States, [redacted]

[4] (U) The term "pen register" is defined in 18 U.S.C. § 3127 as a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication. The term "trap and trace device" is defined in 18 U.S.C. § 3127 as a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

[redacted] If technical devices could not be used to limit collection, the collection required approval by the Attorney General. The Director, NSA could exercise this authority, except when the collection was otherwise regulated, for example, under FISA for communications collected from a wire in the United States.

(U) NSA Initially Used Existing Authorities to Enhance Signals Intelligence (SIGINT) Collection After the September 2001 Terrorist Attacks

~~(TS//SI//NF)~~ On 14 September 2001, NSA Director Hayden used his E.O. 12333 authority to approve a SID CT Product Line request to target [redacted] foreign telephone numbers [redacted] He approved the tasking of the specified numbers, or selectors [redacted] This was an aggressive use of authority because of [redacted] Hayden's 14 September 2001 approval memorandum stated that the purpose of the targeting was to facilitate "dialing analysis/contact chaining."[5] NSA Office of General Counsel (OGC) personnel concurred with the proposed activity, but provided a handwritten note to Hayden stating that chaining was permitted only on foreign numbers, and no U.S. number could be chained without a court order. Collection of the content [redacted] was not addressed in the memorandum. However, other documentation indicates that NSA OGC and SID personnel understood that Hayden also had approved content collection and analysis. NSA OGC personnel told us that Hayden's action was a lawful exercise of his authority under E.O. 12333. In addition, according to NSA's Deputy General Counsel, Hayden had decided by 26 September 2001 that [redacted] would be presumed to be of foreign intelligence value and could be provided to the FBI. Hayden told us that his actions were a "tactical decision" and that he was operating in a unique environment because it was widely believed that more terrorist attacks on U.S. soil were imminent.

~~(S//NF)~~ In late September, Hayden informed Tenet that he had expanded SIGINT operations under E.O. 12333 authority. According to Hayden, Tenet later said that he had explained the NSA's expanded SIGINT operations to Vice President Cheney during a meeting at the White House. On 2 October 2001, Hayden briefed the House Permanent Select Committee on Intelligence on his decision to expand operations under E.O. 12333 and informed members of the Senate Select Committee on Intelligence by telephone.

---

5 (S//SI//NF) Dialing analysis/contact chaining is the process of [redacted] from the communications sent or received by targeted entities.

(U) NSA Explored Options to Improve SIGINT Collection and Address Intelligence Gaps on Terrorist Targets

~~(S//NF)~~ Hayden did not attend the meeting at the White House at which Tenet explained the NSA's expanded SIGINT operations to the Vice President. According to Hayden, Tenet told him that during the meeting the Vice President asked if the IC was doing everything possible to prevent another attack. The Vice President specifically asked Tenet if NSA could do more. Tenet then discussed the matter with Hayden. Hayden told Tenet that nothing more could be done within existing authorities. In a follow-up telephone conversation, Tenet asked Hayden what the NSA could do if it was provided additional authorities. To formulate a response, Hayden met with NSA personnel, who were already working to fill intelligence gaps, to identify additional authorities to support SIGINT collection activities that would be operationally useful and technically feasible. In particular, discussions focused on how NSA might bridge the "international gap," i.e., collection of international communications in which one communicant was within the United States.

(U) In the days immediately after 11 September 2001, the House Permanent Select Committee on Intelligence asked NSA for technical assistance in drafting a proposal to amend FISA to give the President authority to conduct electronic surveillance without a court order to obtain foreign intelligence information. On 20 September 2001, the NSA General Counsel wrote to White House Counsel Gonzales asking if the proposed amendment to FISA had merit. We found no record of a response to the NSA General Counsel's writing and could not determine why the proposal to amend FISA was not pursued at that time.

(U) Hayden said that, in his professional judgment, NSA could not address the intelligence gap using FISA. The process for obtaining FISC orders was slow; it involved extensive coordination and separate legal and policy reviews by several agencies. Although FISA's emergency authorization provision permitted 72 hours of surveillance before obtaining a court order, it did not allow the government to undertake surveillance immediately. Rather, the Attorney General had to ensure that emergency surveillance would satisfy the standards articulated in FISA and be acceptable to the FISC.

[redacted]

[redacted]

(U) Impediments to SIGINT Collection Against Terrorist Targets Were Discussed With the White House

~~(S//NF)~~ Hayden recalled that, after consulting with NSA personnel, he discussed with the White House how FISA constrained NSA collection of communications carried on a wire in the United States. Hayden explained that NSA could not collect from a wire in the United States, without a court order, content or metadata from communications that originated and/or terminated in the United States. Hayden also said that communications metadata do not have the same level of constitutional protection as the content of communications and that access to metadata concerning communications having one end in the United States would significantly enhance NSA's analytic capabilities. Hayden suggested that the ability to collect communications that originated or terminated in the United States without a court order would increase NSA's speed and agility. After two additional meetings with Vice President Cheney to discuss further how NSA collection capabilities could be expanded along the lines described at the White House meeting, the Vice President told Hayden to work out a solution with Counsel to the Vice President David Addington.

(U) Authorization of the President's Surveillance Program

~~(TS//SI//NF)~~ According to Hayden, Addington drafted the first Presidential Authorization of the PSP. Hayden characterized himself as the "subject matter expert," and he said that no other NSA personnel, including the General Counsel, participated in drafting the authorization. Hayden also said that DoJ personnel had not been involved in his discussions with Addington concerning Presidential authorization of the PSP. The PSP came into existence on 4 October 2001, when President Bush signed the Presidential Authorization drafted by Addington. The authorization was entitled: *Presidential Authorization for Specified Electronic Surveillance Activities during a Limited Period to Detect and Prevent Acts of Terrorism within the United States*. Between 4 October 2001 and 8 December 2006, President Bush signed 43 authorizations, exclusive of modifications and other program-related memoranda to the Secretary of Defense.

(U) SIGINT Activities Authorized Under the Program

~~(TS//STLW//SI//OC/NF)~~ The 4 October 2001 Presidential Authorization directed the Secretary of Defense to "use the capabilities of the Department of Defense, including but not limited to the signals intelligence capabilities of the National Security Agency, to collect foreign intelligence by electronic surveillance," provided the surveillance was intended to:

(a) acquire a communication (including but not limited to a wire communication carried into or out of the United States by cable) for which there is probable cause to believe that (b)(1), (b)(3) a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or an agent of such a group; or

(b) acquire, with respect to a communication, header/router/addressing-type information, including telecommunications dialing-type data, but not the contents of the communication, when (i) at least one party to such communication is outside the United States or (ii) no party to such communication is known to be a citizen of the United States.

~~(TS//STLW//SI//OC/NF)~~ The first Presidential Authorization allowed NSA to intercept the content of (b)(1), (b)(3) any communication, including those to, from, or exclusively within the United States, where probable cause existed to believe one of the communicants was engaged in international terrorism. The authorization also allowed the NSA to acquire telephony and Internet metadata where one end of the communication was outside the United States or neither communicant was known to be a U.S. citizen. For telephone calls, metadata generally referred to "dialing-type information" (the originating and terminating telephone numbers, and the date, time, and duration of the call), but not the content of the call. For Internet communications, metadata generally referred to the "to," "from," "cc," "bcc," and "sent" lines of a message, but not the "subject" line or content. (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~ The Secretary of Defense directed NSA, in writing, on 8 October 2001 to execute the authorization to conduct specified electronic surveillance on targets related to (b)(1), (b)(3) international terrorism.[6] Because the surveillance was conducted in the United States, included (b)(1), (b)(3) communications into or out of the United States, and a subset of these communications was to or from persons in the United States, the surveillance otherwise would have required a FISC order. NSA was also allowed to retain, process, analyze, and disseminate intelligence from communications acquired under the Presidential Authorization.

~~(TS//STLW//SI//OC/NF)~~ In addition to allowing the interception of the content of communications into or out of the United States, paragraph (a)(ii) of the first Presidential Authorization allowed NSA to intercept the content of purely domestic communications. Hayden told us he did not realize this until Addington specifically raised the subject during

[6] ~~(S//NF)~~ Although the authorization "was not limited to the signals intelligence capabilities of the National Security Agency," DoD's operational involvement in the PSP was limited to activities undertaken by NSA.

a meeting to discuss renewing the authorization. According to Hayden, he told Addington that NSA would not collect domestic communications because NSA is a foreign intelligence agency, its infrastructure did not support domestic collection, and he would require such a high evidentiary standard to justify intercepting purely domestic communication that such cases might just as well go to the FISC.

(U) Content of the Presidential Authorizations and Department of Justice Certification as to Form and Legality

~~(S//NF)~~ Each of the Presidential Authorizations included a finding to the effect that terrorist groups of global reach possessed the intent and capability to attack the United States, that an extraordinary emergency continued to exist, and that these circumstances constituted an urgent and compelling governmental interest permitting electronic surveillance within the United States for counterterrorism purposes, without judicial warrants or court orders. The primary authorities cited for the legality of the electronic surveillance and related activities were Article II of the Constitution and the 18 September 2001 Authorization for Use of Military Force Joint Resolution (AUMF). The authorizations further provided that any limitation in E.O. 12333 or any other Presidential directive inconsistent with the Presidential Authorizations shall not apply, to the extent of the inconsistency, to the electronic surveillance authorized under the PSP. Each authorization also included the President's determination that, to assist in preserving the secrecy necessary to "detect and prevent acts of terrorism against the United States," the Secretary of Defense was to defer notification of the authorizations and the activities carried out pursuant to them to persons outside the Executive Branch. The President also noted his intention to inform appropriate members of the Senate and the House of Representatives of the program "as soon as I judge that it can be done consistently with national defense needs."

~~(S//NF)~~ Ashcroft certified the first Presidential Authorization as to "form and legality" on 4 October 2001. According to NSA records, this was the same day that Ashcroft was read into the PSP. There was no legal requirement that the Presidential Authorizations of the PSP be certified by the Attorney General or other DoJ officials. Former senior DoJ official Patrick F. Philbin told us he thought one purpose of the certification was to give the program a sense of legitimacy so that it not "look like a rogue operation."

[redacted]

Principal Deputy and Acting Assistant Attorney General Steven G. Bradbury told us that the DoJ certifications served as official confirmation that DoJ had determined that the activities carried out under the program were lawful.

~~(S//NF)~~ Gonzales told us that approval of the program as to form and legality was not required as a matter of law, but he believed that it "added value" to the Presidential Authorization for three reasons. First, NSA was being asked to do something it had not done before, and it was important to assure the NSA that the Attorney General had

approved the legality of the program [redacted] Third, for "purely political considerations," the Attorney General's approval of the program would have value "prospectively" in the event of Congressional or inspector general reviews of the program.

(U) The Presidential Authorizations were issued at intervals of approximately 30 to 60 days. Bradbury said that the main reason for periodically reauthorizing the program was to ensure that the Presidential Authorizations were reviewed frequently to assess the program's value and effectiveness. As the period for each Presidential Authorization drew to a close, the DCI prepared a threat assessment memorandum for the President describing the current state of potential terrorist threats to the United States.

(U) The Threat Assessment Memorandums Supporting Presidential Authorization of the Program

~~(S//NF)~~ From October 2001 to May 2003, the CIA prepared the threat assessment memorandums that supported Presidential authorization and periodic reauthorization of the PSP. The memorandums documented the current threat to the U.S. homeland and to U.S. interests abroad from al-Qa'ida and affiliated terrorist organizations. The first threat assessment memorandum—*The Continuing Near-Term Threat from Usama Bin Ladin*—was signed by the DCI on 4 October 2001.[7] Subsequent threat assessment memorandums were prepared every 30 to 60 days to correspond with the President's reauthorizations.

~~(S//NF)~~ The DCI Chief of Staff, John H. Moseman, was the CIA focal point for preparing the threat assessment memorandums. According to Moseman, he directed the CIA, [redacted] to prepare objective appraisals of the current terrorist threat, focusing primarily on threats to the homeland, and to document those appraisals in a memorandum. [redacted] analysts drew upon all sources of intelligence in preparing their threat assessments. Each of the memorandums focused primarily on the current threat situation and did not routinely provide information concerning previously reported threats or an assessment of the PSP's utility in addressing previously reported threats.

~~(S//NF)~~ After [redacted] completed its portion of the memorandums, Moseman added a paragraph at the end of the memorandums stating that the individuals and organizations involved in global terrorism (and discussed in the memorandums) possessed the capability and intention to undertake further terrorist attacks within the United States. Moseman recalled that the paragraph was provided to him initially by either Gonzales or Addington. The paragraph recommended that the President authorize the Secretary of Defense to employ within the United States the capabilities of DoD, including but not limited to NSA's SIGINT capabilities, to collect foreign intelligence by electronic surveillance. The paragraph described the types of communication and data that would be collected and the

[7] (U) The title of the threat assessment memorandums was changed to *The Global War Against Terrorism* in June 2002.

circumstances under which they could be collected. The draft threat assessment memorandums were reviewed by CIA Office of General Counsel attorneys assigned to [redacted] and CIA Acting General Counsel (Principal Deputy General Counsel), John A. Rizzo. Rizzo told us that the draft memorandums were generally sufficient, but there were occasions when, based on his experience with previous memorandums, he thought that draft memorandums contained insufficient threat information or did not present a compelling case for reauthorization of the PSP. In such instances, Rizzo would request that [redacted] provide additional available threat information or make revisions to the draft memorandums.

~~(S//NF)~~ The threat assessment memorandums were then signed by the DCI and forwarded to the Secretary of Defense to be co-signed. Tenet signed most of the threat memorandums prepared during his tenure as DCI. There were no occasions when the DCI or Acting DCI withheld their signature from the threat assessment memorandums. The threat assessment memorandums were reviewed by DoJ's OLC to assess whether there was "a sufficient factual basis demonstrating a threat of terrorist attacks in the United States for it to continue to be reasonable under the standards of the Fourth Amendment for the President to [continue] to authorize the warrantless searches involved" in the program. OLC then advised the Attorney General whether the constitutional standard of reasonableness had been met and whether the Presidential Authorization could be certified as to form and legality. After review and approval as to form and legality by the Attorney General, the threat assessment memorandums were delivered to the White House to be attached to the PSP reauthorization memorandums signed by the President.

~~(S//NF)~~ Responsibility for drafting the threat assessment memorandums was transferred from [redacted] to the newly-established Terrorist Threat Integration Center in May 2003. This responsibility was retained by TTIC's successor organization, NCTC. The DCI continued to sign the threat assessment memorandums through 15 April 2005. Subsequent memorandums were signed by the Director of National Intelligence or his designee.

(U) Early Revisions to the Presidential Authorizations

~~(TS//STLW//SI//OC/NF)~~ On 2 November 2001, with the first authorization set to expire, President Bush signed a second Presidential Authorization of the PSP. The second authorization cited the same authorities in support of the President's actions, principally the Article II Commander-in-Chief powers and the AUMF. The second authorization also cited the same findings of a threat assessment concerning the magnitude of potential terrorist threats and the likelihood of their occurrence in the future. However, the scope of authorized content collection and metadata acquisition was redefined in the second Presidential Authorization.

~~(TS//STLW//SI//OC/NF)~~ The language of the second Presidential Authorization changed in three respects the scope of collection and acquisition authorized under the PSP. First, the "probable cause to believe" standard for the collection of Internet communications and telephone content was replaced with "based on the factual and

practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe . . .." DoJ, Counsel for Intelligence Policy, James A. Baker told us this change was made by Addington because he believed the terms "probable cause" were "too freighted" with usage in judicial opinions. Baker also said he believed the change to more colloquial language was made because the standard was to be applied by non-lawyers at the NSA. Second, the newly defined standard was to be applied to the belief that the communication "originated or terminated outside the United States . . .." The new language therefore eliminated the authority that existed in the first authorization to intercept the content of purely domestic communications.

~~(TS//STLW//SI//OC/NF)~~ The third change in the scope of PSP collection and acquisition contained in the second Presidential Authorization was the inclusion of an additional (third) category of Internet and telephony metadata that could be acquired:

> (iii) based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are specific and articulable facts giving reason to believe that such communication relates to international terrorism, or activities in preparation therefor.

This language represented an expansion of collection authority to include metadata pertaining to certain communications even when both parties were U.S. persons, as long as there were facts giving reason to believe that the communication was related to international terrorism.

~~(TS//STLW//SI//OC/NF)~~ On 30 November 2001, the President signed a third authorization for the PSP. The third Authorization was virtually identical to the second (2 November 2001) authorization. [redacted]

(b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~ The language in the Presidential Authorization of 9 January 2002 concerning scope of authorized collection and acquisition became the standard for subsequent Presidential Authorizations until the disputed authorization in March 2004, which is discussed later in this report. [redacted]

(b)(1), (b)(3)

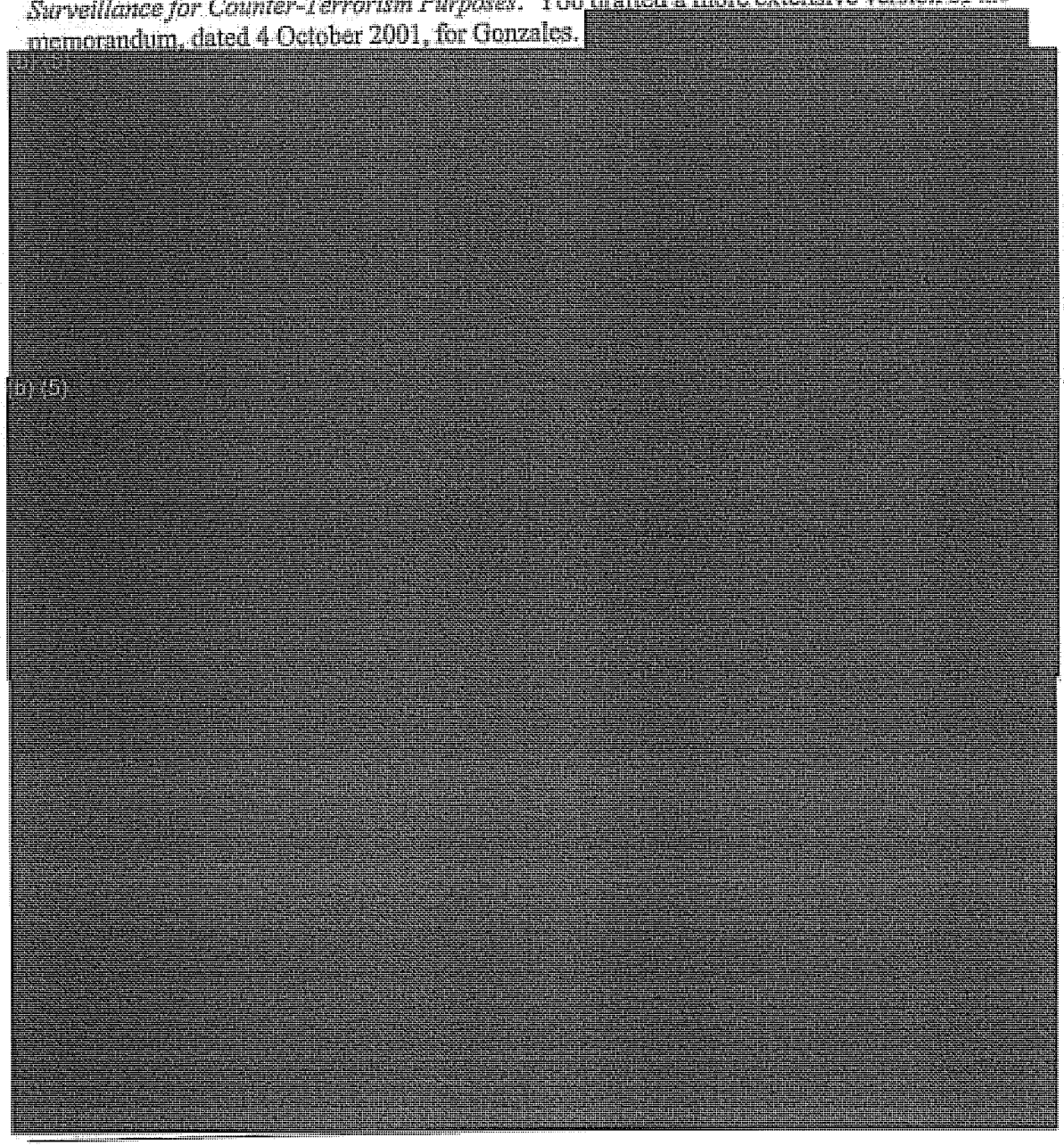
(U) DoJ Office of Legal Counsel Memorandums Supporting Legality of the Program

~~(S//NF)~~ OLC Deputy Assistant Attorney General John Yoo was responsible for drafting the first series of legal memorandums supporting the PSP. Yoo was the only OLC official read into the PSP from the program's inception until he left DoJ in May 2003.

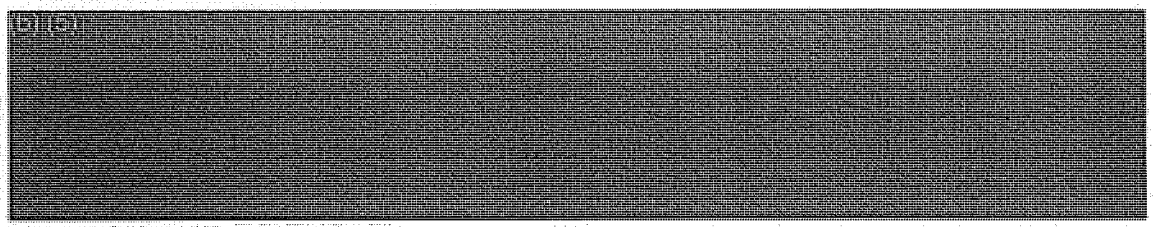
During Yoo's tenure at DoJ, he was one of only three DoJ officials read into the PSP. The other two were Ashcroft and Baker. OLC Assistant Attorney General Jay S. Bybee, Yoo's direct supervisor, was never read into the program.

~~(S//NF)~~ Before the President authorized the PSP on 4 October 2001, Yoo had prepared a memorandum evaluating the legality of a hypothetical electronic surveillance program within the United States to monitor communications of potential terrorists. His memorandum, dated 17 September 2001, was addressed to Deputy White House Counsel Timothy E. Flanigan and was entitled *Constitutional Standards on Random Electronic Surveillance for Counter-Terrorism Purposes*. Yoo drafted a more extensive version of the memorandum, dated 4 October 2001, for Gonzales.

(b) (5)

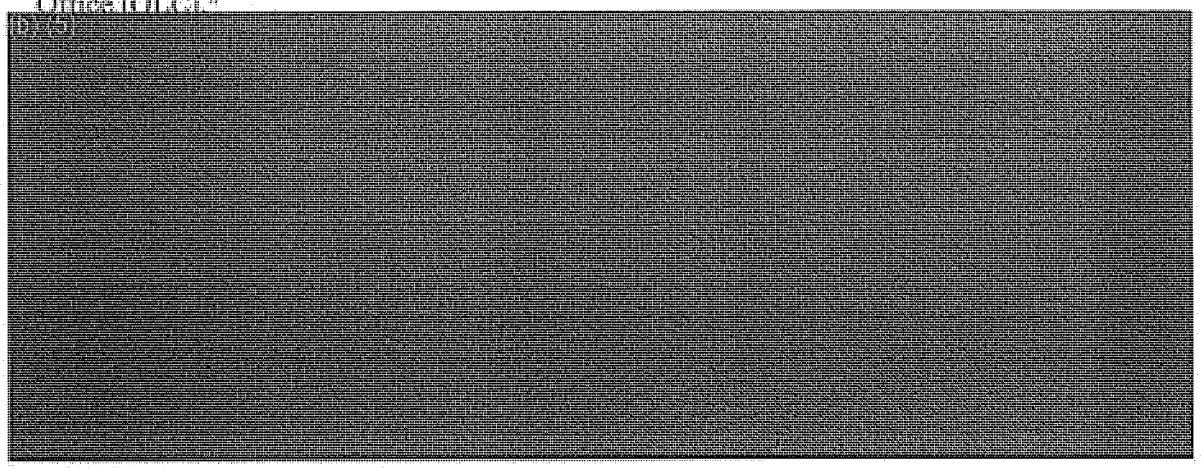


(b)(1)
(b)(3)



~~(S//NF)~~ The first OLC memorandum explicitly addressing the legality of PSP was not drafted until after the program had been formally authorized by the President and after Ashcroft had certified the program as to form and legality. The first OLC opinion directly supporting the legality of the PSP was dated 2 November 2001, and was drafted by Yoo. Yoo acknowledged at the outset of his 2 November memorandum that "[b]ecause of the highly sensitive nature of this subject and the time pressures involved, this memorandum has not undergone the usual editing and review process for opinions that issue from our Office [OLC]."

(b)(1)
(b)(3)



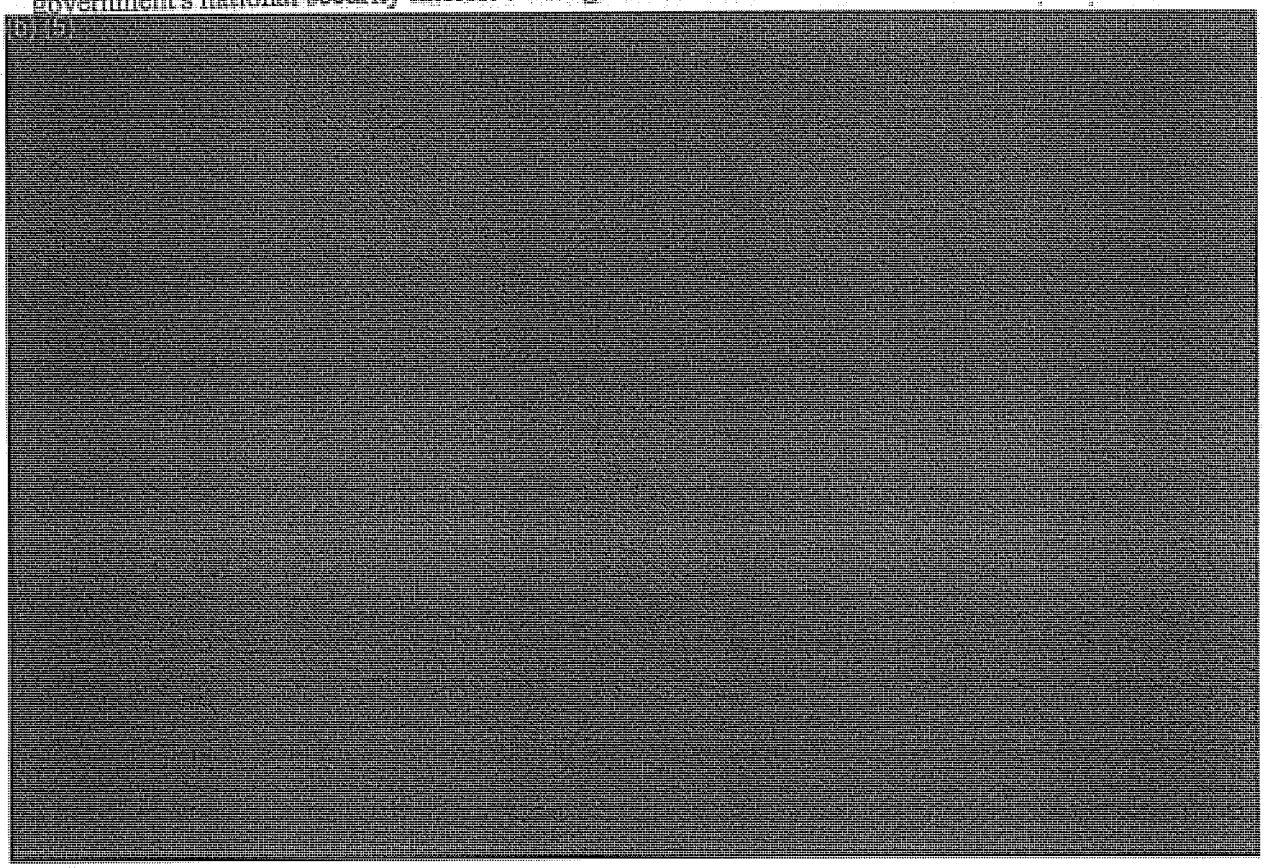
~~(S//NF)~~ Yoo acknowledged in his 2 November 2001 memorandum that the first Presidential Authorization was "in tension with FISA." Yoo stated that FISA "purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence." But Yoo then opined that "[s]uch a reading of FISA would be an unconstitutional infringement on the President's Article II authorities." Citing advice of OLC and DoJ's position as presented to Congress during passage of the USA PATRIOT Act several weeks earlier, Yoo characterized FISA as merely providing a "safe harbor for electronic surveillance," adding that it "cannot restrict the President's ability to engage in warrantless searches that protect the national security."

~~(S//NF)~~ Regarding whether the activities conducted under the PSP could be conducted under FISA, Yoo described the same potential impediments that he had cited in his 4 October memorandum. Noting that the Presidential Authorization could be viewed as a violation of FISA's civil and criminal sanctions in 50 U.S.C. §§ 1809-10, Yoo opined that in this regard FISA represented an unconstitutional infringement on the President's Article II powers. According to Yoo, the ultimate test of whether the government may engage in warrantless electronic surveillance activities is whether such conduct is consistent with the Fourth Amendment, not whether it meets the standards of FISA.

~~(S//NF)~~ Yoo wrote that reading FISA to restrict the President's inherent authority to conduct foreign intelligence surveillance would raise grave constitutional questions which, under the doctrine of constitutional avoidance, would require resolving the issue in a manner that preserves the President's (b) (5) "[U]nless Congress made a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless searches in the national security area—which it has not—then the statute must be construed to avoid such a reading."

~~(TS//SI//NF)~~ Yoo's 2 November 2001 memorandum dismissed Fourth Amendment concerns to the extent that the authorized collection involved non-U.S. persons outside the United States. Regarding those aspects of the program that involved interception of the international communications of U.S. persons within the United States, Yoo asserted that Fourth Amendment jurisprudence allowed for searches of persons crossing U.S. international borders and that interceptions of communications into or out of the United States fell within the "border crossing exception." Yoo further opined that electronic surveillance in "direct support of military operations" did not trigger constitutional protection against illegal searches and seizures, in part because the Fourth Amendment is primarily aimed at curbing law enforcement abuses. Finally, Yoo wrote that the electronic surveillance described in the Presidential Authorizations was "reasonable" under the Fourth Amendment and therefore did not require a warrant, i.e., in this situation the government's national security interest outweighed the individual's privacy interest.

(b) (5)



~~(TS//SI//NF)~~ In October 2002, at Ashcroft's request, Yoo drafted another opinion concerning the PSP. The memorandum, dated 11 October 2002, reiterated the same basic analysis as Yoo's 2 November 2001 memorandum in support of the legality of the PSP.

(b)(5)

[redacted]

(U) IMPLEMENTATION OF THE PRESIDENT'S SURVEILLANCE PROGRAM

(U) NSA Implementation

~~(S//NF)~~ On 4 October 2001, Hayden received the initial Presidential Authorization of the PSP and briefed the NSA SIGINT Director and other key NSA personnel on the authorization. (b)(3)

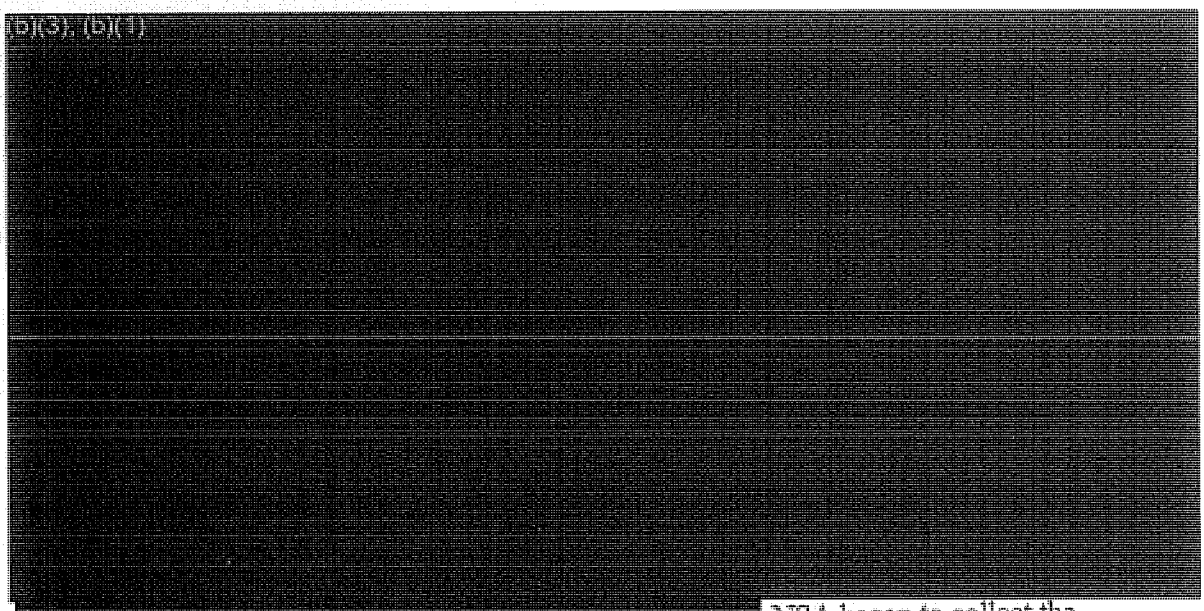
[redacted]

He also said that the NSA General Counsel had reviewed the authorization and concluded that the authorized activities were legal.

(b)(3)

[redacted]

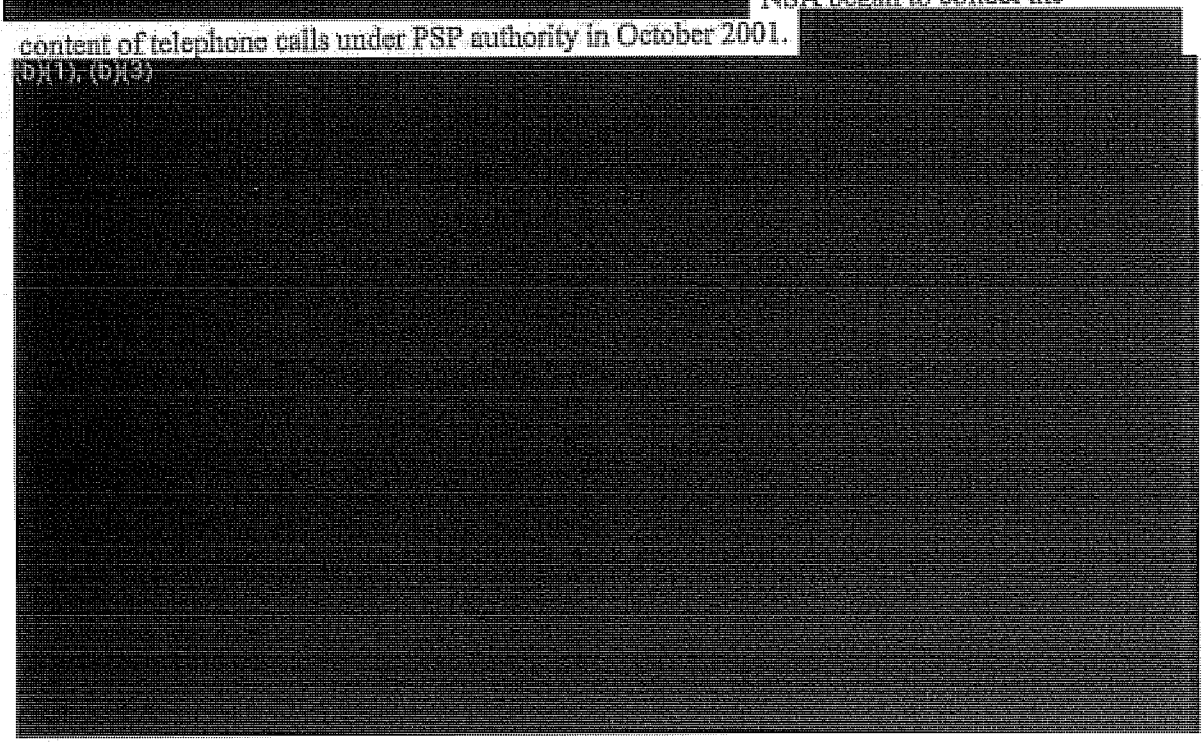
(b)(3), (b)(1)



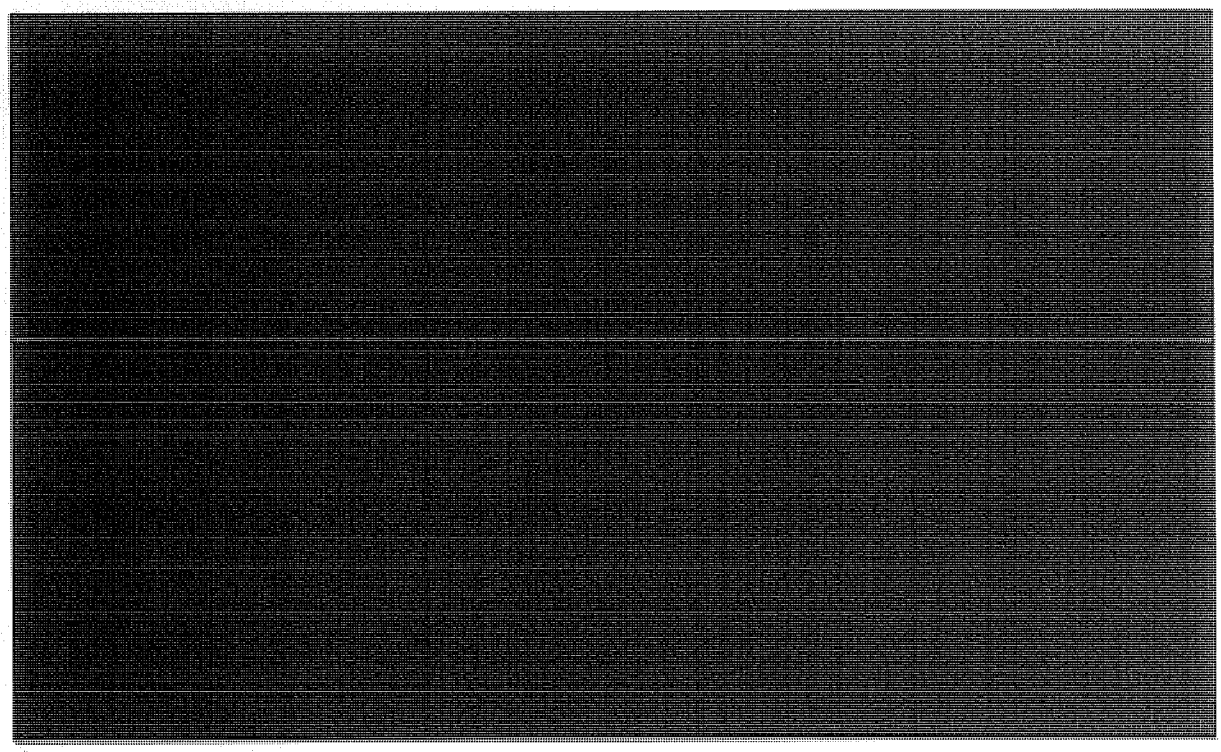
b1,
b3,
b7D,
b7E

NSA began to collect the content of telephone calls under PSP authority in October 2001.

(b)(1), (b)(3)



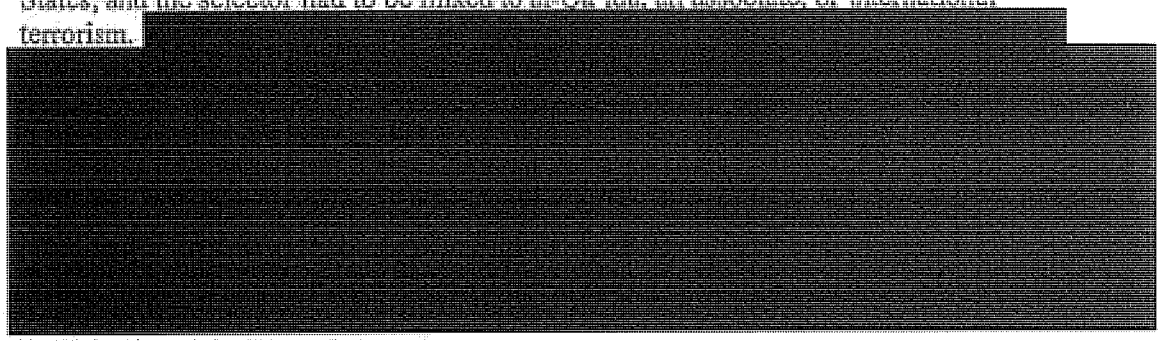
b1,
b3,
b7E



b1, b3, b7E

~~(TS//SI//NF)~~ **Telephone and Internet Communications Content Collection and Analysis**

~~(TS//SI//NF)~~ Content collection and analysis under the PSP was conducted in the same manner as collection and analysis conducted previously by the NSA under E.O. 12333 authority. NSA management applied standard minimization and specially designed procedures to task domestic selectors such as telephone numbers and e-mail addresses. Selectors had to meet two criteria before being tasked under the PSP: the purpose of the collection had to be to prevent and detect terrorist attacks in the United States; and the selector had to be linked to al-Qa'ida, an associate, or international terrorism.



~~(TS//SI//NF)~~ NSA collection managers were responsible for ensuring that telephony and Internet communications selectors were appropriately added or removed from collection. Content collection for domestic selectors was sometimes approved for specific

time periods. Data collected under the PSP were stored in compartmented NSA databases, and access to the databases was strictly controlled.

~~(TS//SI//OC/NF)~~ The majority of targets for content collection under the PSP were foreign telephone numbers and Internet communications addresses. In 2008, NSA reported that [redacted] foreign telephone numbers and in excess of [redacted] foreign Internet communications addresses had been targeted from October 2001 through December 2006. NSA reported in 2008 tha[redacted] domestic telephone numbers and [redacted] domestic Internet communications addresses were targeted for PSP content collection from October 2001 to January 2007. Although targeted domestic telephone numbers and Internet communications addresses were located in the United States, they were not necessarily used by U.S. citizens.

[redacted]

~~(S//NF)~~ PSP program officials told us that the NSA did not seek to collect domestic communications under the PSP. However, NSA managers said that there are no readily available technical means within the [redacted] to guarantee that no domestic calls will be collected. Issues of this kind inevitably arise from time to time in other SIGINT operations, and are not unique to the PSP. Over the life of the program, the NSA reported [redacted] incidents of unintentional collection of domestic communications or non-targeted communications. In such cases, the NSA IG determined that personnel followed established procedures in reporting the incidents, adjusting collection, and purging unauthorized collection records from NSA databases.

~~(TS//SI//NF)~~ NSA analysis of content collected under the PSP involved the same practices and techniques used in analyzing information from other SIGINT operations. Telephone content was made available to NSA analysts through a voice processing system; Internet communications content was available from the database in which it was stored. Analysis involved more than listening to, or reading the content of, a communication and transcribing and disseminating a transcript. Analysis also involved coordinating and collaborating with other IC analysts, applying previous knowledge of the target, and integrating other relevant intelligence.

~~(TS//SI//NF)~~ Telephony and Internet Metadata Collection and Analysis

~~(TS//SI//OC/NF)~~ [redacted] NSA personnel used PSP metadata to perform contact chaining. Although the NSA had the capability to collect bulk telephony and Internet metadata before the PSP, collection was limited because the NSA was not authorized to collect metadata from a wire inside the United States without a court order when one end of the communication was in the United States. NSA could "chain" to, but not through, domestic selectors. Access to large amounts of metadata is required for effective contact chaining, and the PSP increased the data available to NSA analysts and allowed them to perform more thorough contact chaining.

~~(TS//SI//OC/NF)~~ Although NSA analysts could search bulk-collected metadata under the PSP, the analysts' searches were limited to targets that were approved under the standards set forth in the Presidential Authorizations. As such, only a small fraction of the metadata collected under the PSP was ever accessed. In August 2006, the NSA estimated that 0.000025 percent of the telephone records in the PSP database (or one of every four million records) could be expected to be seen by NSA analysts through chaining analysis.

[redacted]

~~(TS//SI//NF)~~ NSA analysts conduct contact chaining by entering a target selector—a telephone number or Internet communication address—in a specialized metadata analysis tool, which searches the metadata and identifies contacts between the selector and other telephone numbers or Internet communications addresses. The resulting contact graph is analyzed for intelligence and to develop investigative leads. [redacted] Although the Presidential Authorizations did not prohibit chaining more than two degrees of separation from the target, NSA analysts determined that it was not analytically useful to do so.

~~(TS//SI//NF)~~ An automated process was created to alert and automatically chain new and potentially reportable telephone numbers using what was called an "alert list." Telephone numbers on the alert list were automatically run against incoming metadata to look for contacts. [redacted]

[redacted]

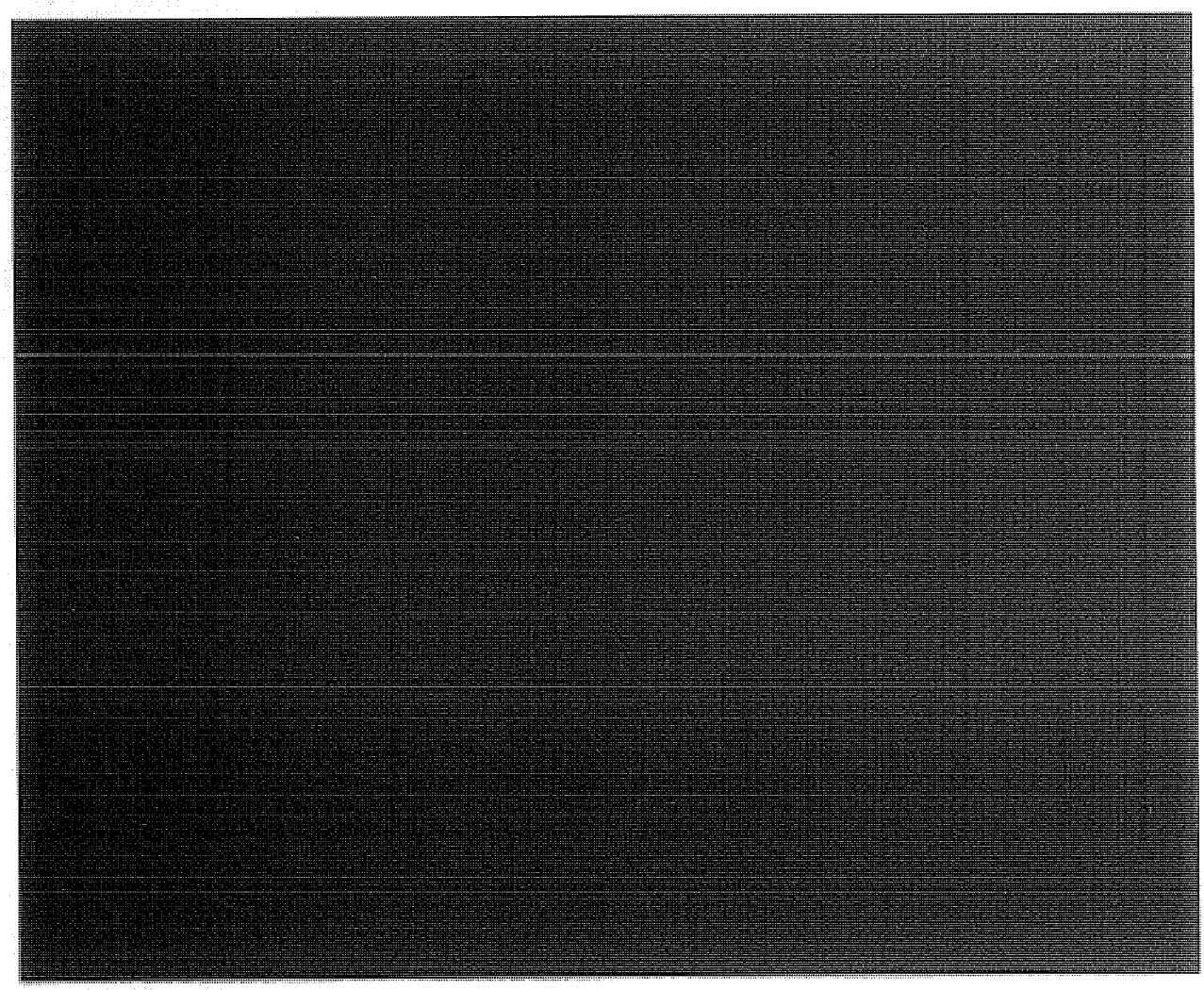
~~(TS//SI//NF)~~ When NSA personnel identified erroneous metadata collection—usually caused by technical problems or inappropriate application of the authorization—they were directed to report the violation or incident through appropriate channels and to delete the collection from all NSA databases. NSA reported three such violations early in the program and took measures to correct them.

(U) NSA Reporting From the President's Surveillance Program

~~(TS//SI//OC/NF)~~ PSP information was disseminated in [redacted] types of reports: "tippers," which provided metadata analysis; content reports, which provided NSA analysis of content collection; [redacted] Tippers were sent to the FBI and the CIA by e-mail on a secure communications network. Some tippers contained "tear line" information that allowed for wider distribution of a sanitized version of the information. From October 2001 through January 2007, the NSA issued [redacted] tippers to the FBI and the CIA.[8]

[redacted]

[8] [redacted]



(U) NSA Managerial Structure and Oversight of the President's Surveillance Program

~~(S//NF)~~ Analysis and reporting associated with the PSP was conducted within SID at NSA's Fort Meade, Maryland headquarters. PSP activities were not conducted at NSA field sites. The Director and Deputy Director of NSA exercised senior operational control and authority over the program. The individual who was SIGINT Director in 2001 told us that, aside from ensuring that the PSP had appropriate checks and balances, she left direct management of the program to the NSA Director, the Deputy Director, and the Office of General Counsel. She noted that Hayden took personal responsibility for the program and managed it carefully.

~~(S//NF)~~ By 2004, specific managerial authorities concerning PSP collection, analysis, and reporting activities had been delegated to the SIGINT Director. The SIGINT Director further delegated managerial authority to the PSP program manager and mission execution responsibilities to the Chief of the CT Product Line. The PSP program manager position was restructured to provide the incumbent authority and responsibility for oversight of PSP

activity across SID, and the PSP program manager was provided additional staff. Over the life of the program, there were five PSP program managers, who reported directly to the SIGINT Director or the Chief of the CT Product Line.

~~(TS//STLW//SI//OC/NF)~~ The NSA supported the operation of the PSP with approximately [redacted] from fiscal years (FYs) 2002 through 2006. Funds were used for the acquisition of [redacted]

(U) NSA PSP Costs From FY 2002 through FY 2006
(dollars in thousands, personnel costs not included)

~~(TS//STLW//SI//OC/NF)~~

[redacted]

(U) NSA Management Controls to Ensure Compliance With Presidential Authorizations

~~(S//NF)~~ NSA management took steps to protect U.S. person information and ensure compliance with the Presidential Authorizations. [redacted]

[redacted]

~~(S//NF)~~ The NSA General Counsel was read into the PSP on 4 October 2001, the day the first Presidential Authorization was signed. On 6 October 2001, the General Counsel provided Hayden and his deputy talking points for use in briefing NSA personnel on the new program's authorities. The talking points included the fact that Hayden had directed the NSA General Counsel and the NSA Associate General Counsel for Operations to review and oversee PSP activities. The NSA Associate General Counsel for Operations provided most of the program oversight before the NSA IG was read into the PSP in August 2002. The Associate General Counsel for Operations oversaw program implementation, reviewed proposed target packages for compliance with the authorizations, and coordinated program-related issues with DoJ.

(U) NSA Inspector General Oversight of the Program

~~(S//NF)~~ The NSA IG and other NSA Office of Inspector General personnel were read into the PSP beginning in August 2002. Over the life of the program, the NSA IG conducted:

- Three investigations in response to specific incidents and violations of the Presidential Authorizations to determine the cause, effect, and remedy.
- Ten reviews to determine the adequacy of management controls to ensure compliance with the authorization and related authorities, assess the mitigation of risk associated with program activities, and identify impediments to meeting the requirements of the authorizations.

~~(TS//SI//NF)~~ Ten of the NSA IG reports included a total of [redacted] recommendations to NSA management to strengthen internal controls and procedures over the PSP. The NSA IG identified no intentional misuse of the PSP. Significant findings from NSA IG reviews of the PSP include the following:

- In 2005, the NSA IG found [redacted] errors when comparing records of domestic telephone and communications selectors approved for PSP content collection with selectors actually on collection. The errors included selectors that were not removed from collection after being detasked, selectors that were not put on collection when approved, and selectors that were mistakenly put on collection due to typographical errors. NSA management took steps to correct the errors and establish procedures to reconcile approved selectors with selectors actually on collection.
- During a 2006 review, the NSA IG found that all items in a randomly selected sample of domestic selectors met Presidential Authorization criteria. Using a statistically valid sampling methodology, the IG concluded with 95 percent confidence that 95 percent or more of domestic

selectors tasked for PSP content collection were linked to al-Qa'ida, its associates, or international terrorist threats inside the United States.

~~(S//NF)~~ In addition to NSA IG report recommendations, in March 2003, the NSA IG recommended to Hayden that he report violations of the Presidential Authorizations to the President. The NSA IG prepared [redacted] Presidential notifications for the NSA Director concerning violations of the authorizations.

~~(S//NF)~~ Beginning in January 2007, violations involving collection activities conducted under PSP authority as well as violations related to former PSP activities that were operating under FISA authority were reported quarterly to the President's Intelligence Oversight Board, through the Assistant to the Secretary of Defense for Intelligence Oversight.

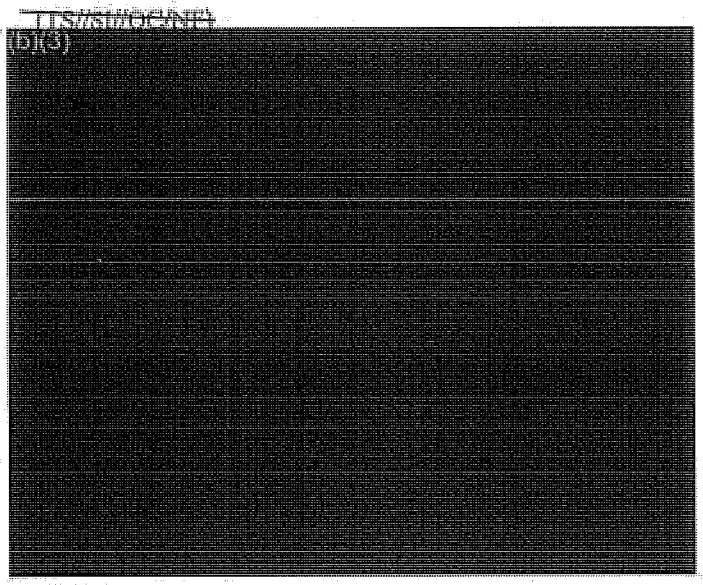
~~(TS//SI//NF)~~ The NSA IG learned in late 2008, that from approximately [redacted] collection of [redacted] All related collection records were purged from NSA databases in 2004; therefore, it was not possible to determine the exact nature and extent of the collection. NSA OIG will close out this incident in its upcoming report to the President's Intelligence Oversight Board.

~~(TS//SI//NF)~~ On 15 January 2009, the DoJ reported to the FISC that the NSA had been using an "alert list" to compare FISA-authorized metadata against telephone numbers associated with counterterrorism targets tasked by the NSA for SIGINT collection. The NSA had reported to the FISC that the alert list consisted of telephone numbers for which NSA had determined the existence of a reasonable, articulable suspicion that the numbers were related to a terrorist organization associated with [redacted] In fact, such a determination had not been made for the majority of the selectors on the alert list. The NSA IG reported this incident to the President's Intelligence Oversight Board, and has provided updates as required. The alert list and a detailed NSA 60-day review of processes related to the business records FISC order were the subject of several recent submissions to the FISC and of NSA briefings to the Congressional oversight committees.

(U) Access to the President's Surveillance Program

[redacted]

(U) PSP Cumulative Clearance Totals
(as of 17 January 2007)



~~(S//NF)~~ Knowledge of the PSP was strictly controlled and limited at the express direction of the White House. Hayden eventually delegated his PSP clearance approval authority for NSA, FBI, and CIA operational personnel to the NSA PSP program manager. Hayden was required to obtain approval from the White House to clear members of Congress, FISC Judges, the NSA IG, and others.

~~(S//NF)~~ The NSA IG was not read into the PSP until August 2002. According to the NSA General Counsel at the time, the President would not allow the IG to be briefed prior to that date. Although Hayden did not recall why the IG had not been cleared earlier, he thought that it would have been inappropriate to clear him when the length of the program was unknown and before operations had stabilized. By August 2002, Hayden and the NSA General Counsel wanted to institutionalize PSP oversight with the involvement of the NSA IG. Hayden recalled having to "make a case" to the White House to have the NSA IG read in. The ODNI IG found that ODNI oversight of the PSP was limited by ODNI oversight personnel not being provided timely access to the program.

(U) Congressional Briefings on the Program

~~(TS//SI//NF)~~ On 25 October 2001, Hayden conducted a briefing on the PSP for the Chairman and the Ranking Member of the House Permanent Select Committee on Intelligence, Nancy P. Pelosi and Porter J. Goss; and the Chairman and the Vice Chairman of the Senate Select Committee on Intelligence (SSCI), D. Robert Graham and Richard C. Shelby. Between 25 October 2001 and 17 January 2007, Hayden and current NSA Director Alexander, sometimes supported by other NSA personnel, conducted

49 briefings to members of Congress and their staff. Hayden told us that during the many PSP briefings to members of Congress, no one ever suggested that the NSA should stop the program. Hayden emphasized that he did more than just "flip through slides" during the briefings, which lasted as long as attendees had questions.

(U) Foreign Intelligence Surveillance Court Briefings on the Program

~~(TS//SI//OC/NF)~~ On 31 January 2002, the FISC Presiding Judge Royce Lamberth became the first member of the court to be read into the PSP. He was briefed on the program after James Baker, the head of DoJ's Office of Intelligence Policy and Review (OIPR) (b) (5) [redacted] Lamberth's briefing was conducted at the DoJ and was attended by Ashcroft, Hayden, Mueller, Yoo, and Baker.

~~(TS//SI//OC/NF)~~ Ashcroft provided Lamberth a brief summary of the President's decision to create the PSP, and Ashcroft stated that he had determined, based upon the advice of John Yoo, an attorney in DoJ's Office of Legal Counsel (OLC), that the President's actions were lawful under the Constitution. Ashcroft also emphasized to Lamberth that the FISC was not being asked to approve the program. Following Ashcroft's summary, Hayden described for Lamberth how the program functioned operationally, Yoo discussed legal aspects of the program, and Baker proposed procedures for handling international terrorism FISA applications that contained PSP-derived information. For the next four months, until the end of his term in May 2002, Lamberth was the only FISC judge read into the PSP.

~~(TS//SI//OC/NF)~~ Judge Colleen Kollar-Kotelly succeeded Lamberth as the FISC Presiding Judge and was briefed on the PSP on 17 May 2002. The briefing was similar in form and substance to that provided to Lamberth. In response to several questions from Kollar-Kotelly about the scope of the President's authority to conduct warrantless surveillance, DoJ prepared a letter to Kollar-Kotelly, signed by Yoo, that, according to Kollar-Kotelly, "set out a broad overview of the legal authority for conducting [the PSP], but did not analyze the specifics of the [PSP] program." The letter, which Kollar-Kotelly reviewed at the White House but was not permitted to retain, essentially replicated Yoo's 2 November 2001 memorandum regarding the legality of the PSP. Kollar-Kotelly was the only sitting FISC judge read into the PSP until January 2006, when the other FISC judges were read in.

~~(TS//SI//OC/NF)~~ Baker was read into the PSP only after he came upon "strange, unattributed" language in a FISA application that suggested the existence of a compartmented program. (b) (5) [redacted] As noted, eventually Lamberth, and later his successor, Kollar-Kotelly, were read in. The DoJ IG believes that not having OIPR officials and members of the FISC read into the PSP, while program-derived information was being disseminated as investigative leads to the FBI and finding its way into FISA

applications, put at risk the DoJ's important relationship with the FISC. The DoJ IG agrees with Baker's assessment that, as the government's representative before the FISC, good relations between the DoJ and the FISC depend on candor and transparency.

(U) FBI Participation in the President's Surveillance Program

~~(TS//SI//NF)~~ As a user of PSP-derived information, the FBI disseminated leads—tippers—to FBI field offices. Tippers primarily consisted of domestic telephone numbers and Internet communications addresses that NSA analysts had determined through metadata analysis were connected to individuals involved with al-Qa'ida or its affiliates. Domestic telephone numbers represented the overwhelming majority of PSP-derived information contained in tippers. Tippers also provided information derived from content collection under the PSP.

~~(TS//SI//NF)~~ The FBI's principal objective during the earliest months of the PSP was to disseminate program information to FBI field offices for investigation while protecting the source of the information and the methods used to collect it. The FBI initially assigned responsibility for this to its Telephone Analysis Unit (TAU), which developed procedures to disseminate information from NSA's PSP reports in a non-compartmented, Secret-level format. The resulting [redacted] Electronic Communications (ECs) included restrictions on how the information could be used, i.e., FBI field offices were to use the information "for lead purposes only" and not use the information in legal or judicial proceedings. b1, b3, b7E

~~(S//NF)~~ The FBI's participation in the PSP evolved over time as the program became less a temporary response to the September 11 attacks and more a permanent surveillance capability. To improve the effectiveness of its participation in the program, the FBI initiated the [redacted] project in [redacted] to manage its involvement in the PSP. In February 2003, the FBI assigned a team of FBI personnel—"Team 10"—to work full-time at the NSA to manage the FBI's participation in the program. b1, b3, b7E

~~(TS//SI//NF)~~ Team 10's primary responsibility was to disseminate PSP information through [redacted] ECs to FBI field offices for investigation or other purposes. However, over time, Team 10 began to participate in the PSP in other ways. For example, Team 10 occasionally submitted telephone numbers and Internet communications addresses to the NSA to be searched against the bulk metadata collected under the PSP. The NSA conducted independent analysis to determine whether telephone numbers or Internet communications addresses submitted by Team 10 met the standards established by the Presidential Authorizations. Team 10 also regularly contributed to NSA's PSP process by reviewing draft reports and providing relevant information from FBI databases. b1, b3, b7E

~~(S//NF)~~ FBI field offices were not required to investigate every tipper disseminated by Team 10 under the [redacted] project. Rather, the type of lead that the [redacted] EC assigned—"action," "discretionary," or "for information"—drove the field office's b1, b3, b7E

response to a tipper.[9] The vast majority of FBI investigative activity related to PSP information involved responding to [redacted] telephone number tippers that assigned action leads. Team 10 generally assigned action leads for telephone numbers that were not already known to the FBI or telephone numbers that Team 10 otherwise deemed a high priority, such as a number that had a relationship to a major FBI investigation. From approximately [redacted] when [redacted] was established, to [redacted] action leads instructed field offices to obtain subscriber information for the telephone numbers within its jurisdiction and to conduct any "logical investigation to determine terrorist connections." Some agents complained that action leads lacked guidance about how to make use of the tippers, which was of particular concern because agents were not confident that [redacted] communications provided sufficient predication to open national security investigations. b1, b3, b7E

~~(TS//SI//NF)~~ Two changes to FBI procedures in 2003 addressed some FBI agents' concerns. [redacted] FBI Headquarters assumed responsibility from field offices for issuing national security letters (NSLs) to obtain subscriber information about PSP-tipped telephone numbers and Internet communications addresses. [redacted] the Attorney General issued new guidelines for FBI national security investigations that created a new category of investigative activity called a "threat assessment." Under a threat assessment, FBI agents are authorized to investigate or collect information on individuals, groups, and organizations of possible investigative interest without opening a preliminary or full national security investigation. Beginning [redacted] action leads assigned by [redacted] metadata tippers instructed field offices to conduct threat assessments and advised that FBI headquarters would issue NSLs to obtain subscriber information. b1, b3, b7E

~~(S//NF)~~ In general, an FBI threat assessment involved searching several FBI, public, and commercial databases for information about the tipped telephone number, and requesting that various state and local government entities conduct similar searches. Sometimes these searches identified the subscriber to the telephone number before FBI Headquarters obtained the information with an NSL. In other cases, the threat assessments continued after the field office received the NSL results.

~~(S//NF)~~ The [redacted] leads frequently were closed after conducting a threat assessment interview with the subscriber and determining that there was no nexus to terrorism or threat to national security. In other cases, the leads were closed based solely on the results of database checks. b1, b3, b7E

~~(S//NF)~~ Beginning [redacted] FBI field offices were required to report the results of their threat assessments to FBI headquarters. FBI field offices typically reported all of the information that was obtained about the tipped telephone numbers, including the details of any subscriber interviews, and then stated that the office had determined that the b1, b3, b7E

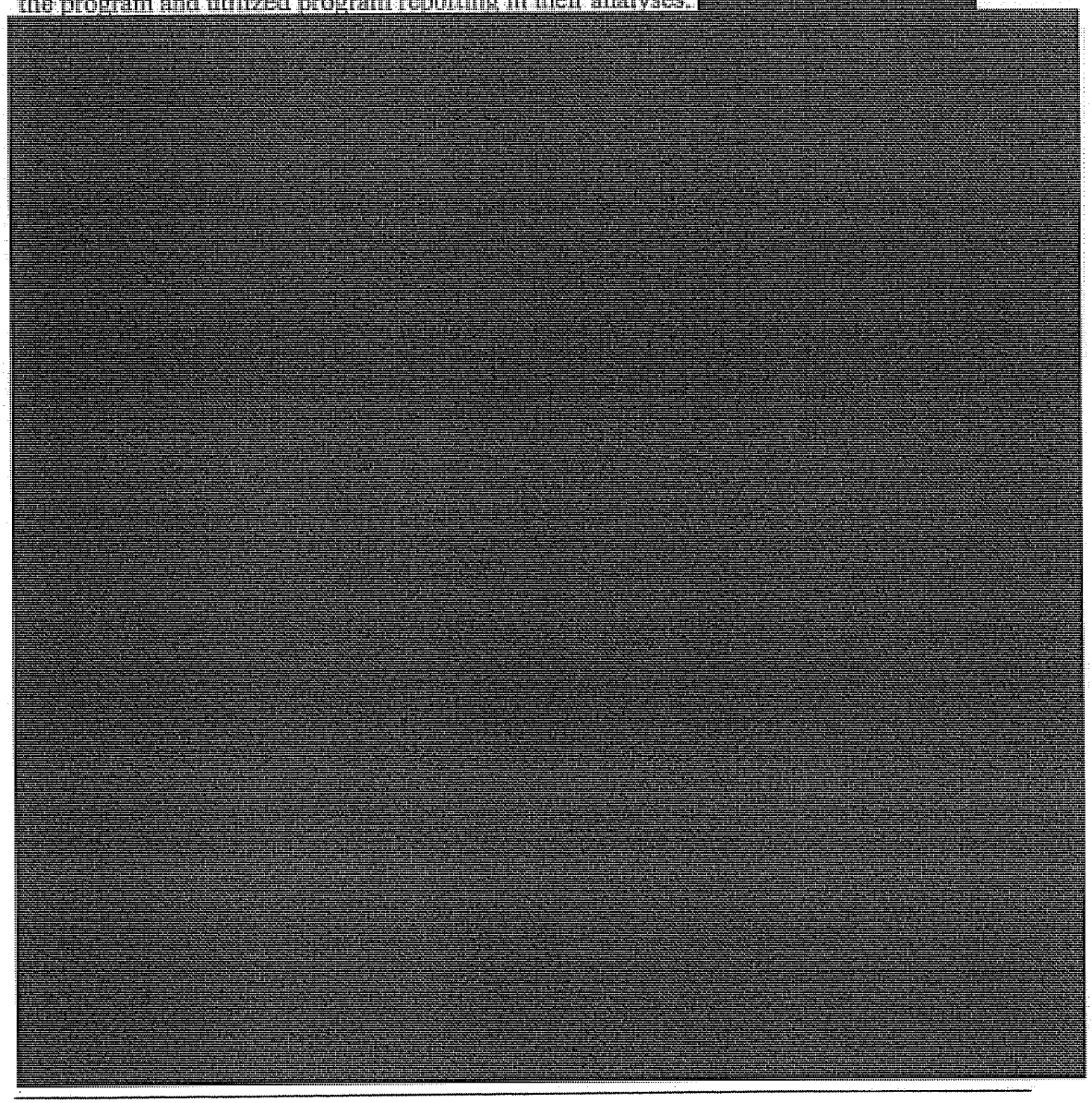
---

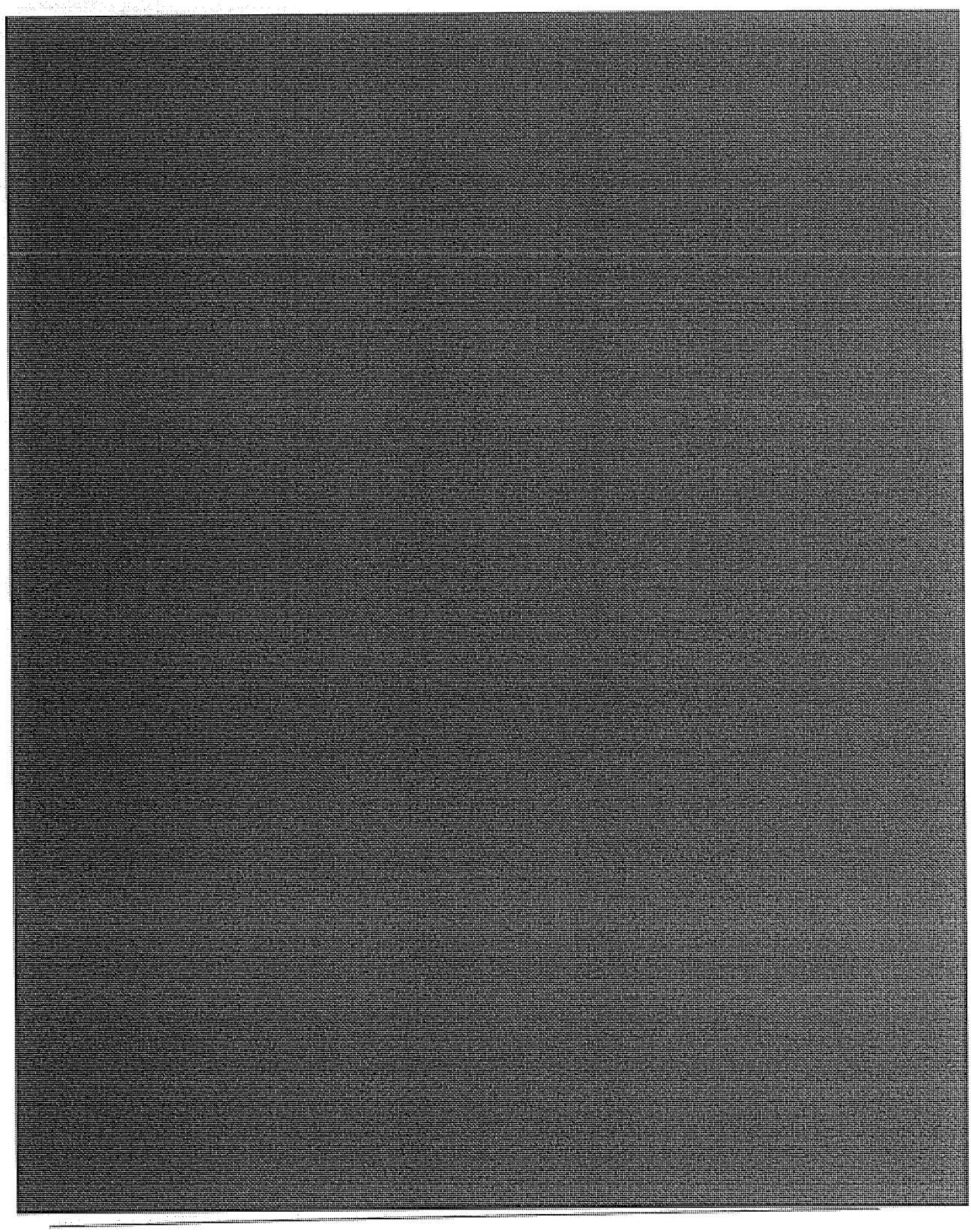
[9] ~~(S//NF)~~ An action lead instructs an FBI field office to take a particular action in response. A discretionary lead allows the field office to make a determination whether the information provided warrants investigative action. A field office is not expected to take any specific action on a for information lead.

telephone number did not have a nexus to terrorism and considered the lead closed. Much less frequently, field offices reported that a preliminary investigation was opened. Regardless of whether any links to international terrorism were identified in a threat assessment, the results of the threat assessments and the information that was collected about subscribers generally were reported to FBI headquarters and uploaded to FBI databases.

(U) CIA Participation in the President's Surveillance Program

~~(S//NF)~~ CIA analysts and targeters, as PSP consumers, requested information from the program and utilized program reporting in their analyses.





[redacted]

(U) NCTC Participation in the President's Surveillance Program

~~(TS//SI//NF)~~ The ODNI IG found that the ODNI's primary role in the PSP was the preparation of the threat assessments that summarized the al-Qa'ida threat to the United States and were used to support periodic reauthorization of the program. The ODNI IG found that the threat assessments were drafted by experienced NCTC personnel who prepared the documents in a memorandum style following an established DoJ format. The ODNI IG also determined that the ODNI threat assessments were prepared using evaluated intelligence information chosen from a wide variety of IC sources. ODNI personnel said that during the period when the ODNI prepared the threat assessments, the IC had access to fully evaluated intelligence that readily supported an assessment that al-Qa'ida remained a significant threat to the United States.

~~(TS//SI//NF)~~ [redacted] The NCTC analysts told us that PSP information was subject to stringent security protections [redacted]

~~(S//NF)~~ The NCTC analysts said that they handle NSA surveillance information, including PSP information, consistent with the standard rules and procedures for handling NSA intelligence information including minimization of U.S. person identities. On those occasions when the NCTC analysts knew that a particular NSA intelligence product was derived from the PSP, the analysts told us they reviewed program information in the same manner as other incoming NSA intelligence products. If appropriate, NCTC analysts then incorporated the PSP information into analytical products being prepared for the Director of National Intelligence (DNI) and other senior intelligence officials. They identified the President's Terrorism Threat Report and the Senior Executive Terrorism Report as examples of the types of finished intelligence products that would, at times, contain PSP information.

(U) The President's Surveillance Program and the Foreign Intelligence Surveillance Court

~~(TS//SI//NF)~~ DoJ, initially with the FISC's concurrence and later at the court's direction, developed and implemented procedures—referred to as "scrubbing" procedures—to account for and make the court aware of instances when PSP-derived information was included in FISA applications. Lamberth required that all FISA applications that contained PSP-derived information, or that would result in simultaneous collection against particular targets under both the PSP and a FISC order, be filed with him only. Baker told us that Lamberth wanted to be informed of applications that contained PSP information and of dual coverage situations. According to Baker, the scrubbing procedures were a means of meeting his ethical duty of candor to the FISC without disclosing the existence of the PSP to uncleared judges.

~~(TS//SI//NF)~~ DoJ effectuated the scrubbing procedures by compiling lists of information contained in initial and renewal FISA applications that was attributed to the NSA and of all facilities targeted for electronic surveillance in the applications. These lists were sent to the NSA to determine whether any of the NSA-attributed information was PSP-derived and whether any of the facilities also were targeted under the PSP. The NSA communicated the results back to DoJ, which then filed the applications with the FISC consistent with the scrubbing procedures.

~~(TS//SI//NF)~~ Kollar-Kotelly continued the procedures that had been developed by Baker and agreed to by Lamberth for handling FISA applications that contained PSP-derived information. However, Kollar-Kotelly required DoJ to excise from FISA applications any information obtained or derived from the PSP. But Kollar-Kotelly also instructed Baker to alert her to any instances where an application's basis for the requisite probable cause showing under FISA was weakened by excising PSP information. In such cases, Kollar-Kotelly would then assess the application with the knowledge that additional relevant information had been excised.

~~(TS//SI//OC/NF)~~ Kollar-Kotelly also instructed DoJ to discontinue the practice employed under Lamberth of including in applications a descriptive phrase associated with [redacted] as a means of indicating that facilities targeted by the applications were also targeted under the PSP. Baker told us that while Kollar-Kotelly understood that instances of dual coverage would occur, she did not want to appear to judicially sanction PSP coverage. b1, b3, b7E

~~(TS//SI//NF)~~ In March 2004, Kollar-Kotelly was informed of operational changes made to the PSP following a dispute between DoJ and the White House about the legal basis for certain aspects of the program. Kollar-Kotelly responded by imposing an additional scrubbing requirement to further ensure, to the extent possible, that PSP-derived information was not included in FISA applications. The FBI, in coordination with DoJ and NSA, was to determine whether a facility included in a FISA application—not just a targeted telephone number or Internet communication address—also appeared in a PSP report. Kollar-Kotelly permitted any such facility to remain in the application if it could be

demonstrated that the FBI had developed, independent of the PSP, an investigative interest in the facility, or that the FBI inevitably would have identified the facility in question through normal investigative steps. An OIPR official who was responsible for discussing such cases with Kollar-Kotelly told us that the judge generally accepted DoJ's assessment that there was a non-PSP investigative basis for a facility in question, or that the facility inevitably would have been discovered even in the absence of PSP-derived leads to the FBI.

~~(S//NF)~~ Implementing the scrubbing procedures, both under Lamberth and Kollar-Kotelly, was a complicated and time-consuming endeavor for OIPR staff. Baker, who until March 2004 was the only individual in OIPR read into the PSP, found himself having to ask OIPR attorneys to compile information about their cases, and sometimes to make changes to their FISA applications, without being able to provide an explanation other than that he had spoken to the Attorney General and the FISC about the situation. Baker regularly told attorneys that they did not have to sign applications that they were not comfortable with, and, in some instances, international terrorism cases had to be reassigned for this reason.

~~(S//NF)~~ The situation was further complicated by the fact that, until August 2003, only one of the two DoJ officials authorized by statute to approve FISA applications—Attorney General Ashcroft and Deputy Attorney General Larry Thompson—was read into the PSP. Thompson, who served as Deputy Attorney General from May 2001 to August 2003, was never read into the PSP, despite Ashcroft's request to the White House.

~~(TS//SI//NF)~~ Similarly, Kollar-Kotelly, who by November 2004 was handling approximately [redacted] percent of all FISA applications as a result of her requirement that scrubbed applications be filed with her only, made unsuccessful requests for additional FISC judges to be cleared for the program. Kollar-Kotelly decided in November 2004 that in view of the scrubbing procedures that were in operation, international terrorism FISA applications could be decided by other judges based on the information contained in the applications.

~~(TS//SI//NF)~~ DoJ, together with the FBI and the NSA, continue to apply the scrubbing procedures to international terrorism FISA applications. Since January 2006, all members of the FISC have been briefed on the PSP and all of the judges handle applications that involve the issue of PSP-derived information. Although compliance with the scrubbing procedures has been burdensome, we did not find instances when the government was unable to obtain FISA surveillance coverage on a target because of the requirement. However, the DoJ IG concluded that once the PSP began to affect the functioning of the FISA process, OIPR and the FISC effectively became part of the PSP's operations, and more OIPR staff and FISC judges should have been read into the PSP to address the impact. Instead, access to the PSP was limited for years to a single OIPR official and one FISC judge.

(U) Discovery Issues Associated With the President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ DoJ was aware as early as (b)(1), (b)(3) that information collected under the PSP could have implications for DoJ's litigation responsibilities under Rule 16 of the Federal Rules of Criminal Procedure and *Brady v. Maryland*, 373 U.S. 83 (1963). Analysis of the discovery issue was first assigned to Yoo in [redacted] (b)(1), (b)(3), (b)(6), (b)(7)

b1, b3, b6, b7C, b7E

[redacted] (b)(1), (b)(3)

b1, b3, b6, b7C b7E

~~(S//NF)~~ No DoJ attorneys with terrorism prosecution responsibilities were read into the PSP until mid-2004, and as a result, DoJ did not have access to the advice of attorneys who were best equipped to identify and examine discovery issues associated with the PSP. The DoJ IG believes that, since then, DoJ has taken steps to respond (b)(1), (b)(3) [redacted] to [redacted] discovery motions (b)(1), (b)(3) [redacted] DoJ's responses to the discovery motions involve the use of the Classified Information Procedures Act, 18 U.S.C. App. 3, to file *ex parte* in camera pleadings with federal courts to describe potentially responsive PSP-derived information. [redacted] (b)(3), (b)(1)

~~(S//NF)~~ [redacted] the DoJ IG recommends that DoJ assess its discovery obligations regarding PSP-derived information in international terrorism prosecutions, carefully consider whether it must re-examine past cases to see whether potentially discoverable but undisclosed Rule 16 or *Brady* material was collected by the NSA, and take appropriate steps to ensure that it has complied with its discovery obligations in such cases. The DoJ IG also recommends that DoJ, in coordination with the NSA, implement a procedure to identify PSP-derived information that may be associated with international terrorism cases

currently pending or likely to be brought in the future and evaluate whether such information should be disclosed in light of the government's discovery obligations under Rule 16 and *Brady*.

(U) LEGAL REASSESSMENT OF THE PRESIDENT'S SURVEILLANCE PROGRAM (2003 – 2004)

~~(TS//SI//NF)~~ Concern Over the [redacted] Collection

(b)(1), (b)(3)

~~(TS//SI//NF)~~ Yoo was the sole OLC attorney who advised Ashcroft and White House officials on the PSP from the program's inception in October 2001 through Yoo's resignation from DoJ in May 2003. Upon Yoo's departure, Patrick Philbin was selected by the White House to be read into the PSP to assume Yoo's role as advisor to the Attorney General concerning the program.

~~(TS//SI//NF)~~ Philbin told us that when he reviewed Yoo's legal memorandums about the PSP, he realized that Yoo had omitted from his analysis any reference to the FISA provision allowing the interception of electronic communications without a warrant for a period of 15 days following a Congressional declaration of war. (See 50 U.S.C. § 1811.) Philbin stated that Yoo's OLC opinions were premised on the assumption that FISA did not expressly apply to wartime operations, an assumption that from Philbin's perspective made the opinions "problematic."

(b)(1), (b)(3)

[redacted]

(b) (5), (b)(1), (b)(3)

~~(S//NF)~~ In August 2003, Philbin told Ashcroft that there were problems with the legal analysis supporting the PSP but probably not with the conclusions reached, and he therefore advised Ashcroft to continue to certify the program "as to form and legality." Philbin also recommended that a new OLC memorandum assessing the legality of the PSP be drafted, and with Ashcroft's concurrence he began drafting the memorandum.

(U) A New Legal Basis for the Program Is Adopted

~~(S//NF)~~ Goldsmith was sworn in as the Assistant Attorney General for OLC on 6 October 2003, replacing Bybee, who had left that position several months earlier to serve as a judge on the U.S. Court of Appeals for the Ninth Circuit. Philbin told us that he pressed hard to have Goldsmith read into the PSP, and that Addington told Philbin he would have to justify the request before Addington would take it to the President for a decision. Addington subsequently read Goldsmith into the program on 17 November 2003.

~~(TS//SI//NF)~~ After reviewing Yoo's memorandums and Philbin's new draft analysis of the PSP, Goldsmith agreed with Philbin's concerns about the existing legal analysis supporting the program.

(b) (5), (b)(1), (b)(3)

~~(S//SI//NF)~~

(b) (5), (b)(1), (b)(3)

(b) (5), (b)(1), (b)(3)

(b)(5), (b)(1), (b)(3)

~~(TS//SI//NF)~~ Goldsmith concluded that the NSA's interception of (b)(5), (b)(1), (b)(3) did not comply with FISA's requirement to obtain judicial authorization, and did not fall within any of the exceptions to this requirement. Goldsmith later wrote in a 6 May 2004 legal memorandum reassessing the legality of the program that a proper analysis of the PSP "must not consider FISA in isolation" but rather must consider whether Congress, by authorizing the use of military force against al-Qa'ida, also "effectively exempts" such surveillance from FISA. Goldsmith believed that this reading of the AUMF was correct because the AUMF authorized the President to use "all necessary and appropriate force" against the enemy that attacked the United States on 11 September 2001, and to "prevent any future acts of international terrorism against the United States" by such enemy—authority that has long been recognized to include the use of SIGINT as a military tool. Alternatively, Goldsmith reasoned that even if the AUMF did not exempt surveillance under the program from the restrictions imposed by FISA, the question was sufficiently ambiguous to warrant the application of the doctrine of constitutional avoidance, and therefore should be construed not to prohibit the activity.[11]

(b)(5), (b)(1), (b)(3)

[11] ~~(TS//SI//NF)~~ (b)(5), (b)(1), (b)(3)

~~(TS//SI//NF)~~ In late 2003, Philbin and Goldsmith were the only two DoJ officials in a position to brief the Attorney General and White House officials on the status of their legal reassessment and its potential ramifications for the operation of the program. Goldsmith advised Ashcroft that, despite concerns about the program, Ashcroft should certify the 9 December 2003 Presidential Authorization. Goldsmith later advised Ashcroft to certify the 14 January 2004 authorization as well. Goldsmith told us that he made these recommendations to Ashcroft with the caveat that although he believed Yoo's memorandums to be flawed, Goldsmith had not yet concluded that the program itself was illegal.

(U) Department of Justice Officials Convey Concerns About the Program to the White House

~~(TS//SI//NF)~~ In December 2003, Goldsmith and Philbin met with Addington and Gonzales at the White House to express their growing concerns about the legal underpinnings for the program. Goldsmith said he told them that OLC was not sure the program could survive in its current form. According to Goldsmith's contemporaneous notes of these events, these discussions did not contemplate an interruption of the program, although the White House officials represented that they would "agree to pull the plug" if the problems with the program were found to be sufficiently serious. Goldsmith told us that the White House—typically through Addington—told him "several times" that it would halt the program if DoJ found that it could not be legally supported.

~~(TS//SI//NF)~~ On 18 December 2003, Goldsmith met again with Addington and Gonzales and wrote in his notes that during this meeting he conveyed with "more force" his "serious doubts and the need to get more help to resolve the issue [as soon as possible]." Goldsmith told us that during this meeting he also asked to have Deputy Attorney General Comey read into the program. According to Goldsmith's notes, Addington and Gonzales "bristle[d]" at that suggestion. Goldsmith told us that he requested that Comey be read in because he believed he would need Comey's assistance to help "make the case" to the White House that the program was legally flawed. In addition, he said he wanted Comey read in because, as the Deputy Attorney General, Comey was Philbin's direct supervisor.

~~(TS//SI//NF)~~ Goldsmith's efforts to gain the White House's permission to have additional attorneys, and especially Comey, read into the program continued through January 2004. According to Goldsmith's notes, both Addington and Gonzales pressed Goldsmith on his reason for the request and continued to express doubt that additional DoJ personnel were needed. However, in late January 2004 the White House agreed to allow Comey to be read in, and Comey was briefed into the PSP on 12 March 2004 by Hayden.

~~(S//NF)~~ After his briefing, Comey discussed the program with Goldsmith, Philbin, and other DoJ officials, and agreed that the concerns with Yoo's legal analysis were well-founded.[12] Comey told us that of particular concern to him and Goldsmith was the notion that Yoo's legal analysis entailed ignoring an act of Congress, and doing so without full Congressional notification.

~~(TS//SI//NF)~~ Comey told us that in early March 2004 the sense at DoJ was that "we can get there" with regard to (b)(1), (b)(3) albeit by using an aggressive legal analysis. However, he agreed with Goldsmith's conclusion that (b)(1), (b)(3) would require (b)(1), (b)(3)

(U) Conflict Between the Department of Justice and the White House Over the Program

(U) Comey told us that he met with Ashcroft for lunch on 4 March 2004 to discuss the PSP, and that Ashcroft agreed with Comey and the other DoJ officials' assessment of the potential legal problems with the program. Three hours after their lunch meeting, Ashcroft became ill and was admitted to the George Washington University Hospital.[13] On 5 March 2004, Goldsmith advised Comey by memorandum that under the circumstances of Ashcroft's medical condition and hospitalization, a "clear basis" existed for Comey to exercise the authorities of the Attorney General allowed by law as Deputy Attorney General or Acting Attorney General. The "cc" line of Goldsmith's memorandum to Comey indicated that a copy of the memorandum was sent to Gonzales.

~~(TS//SI//NF)~~ On 5 March 2004—six days before the Presidential Authorization then in effect was set to expire—Goldsmith and Philbin met with Addington and Gonzales at the White House to again convey their concerns about the PSP. (b) (5), (b)(1), (b)(3) Later that day, Gonzales called Goldsmith to request a letter from OLC stating that Yoo's prior OLC opinions "covered the program." Philbin told us that Gonzales was not requesting a new opinion that the program itself was legal, but only a letter stating that the prior opinions had concluded that it was.

---

[12] ~~(TS//SI//OC/NF)~~ The other officials included Counsel for Intelligence Policy Baker, Counselor to the Attorney General Levin, and Comey's Chief of Staff Chuck Rosenberg. Both Levin and Rosenberg had been read into the PSP while at the FBI. Comey also discussed DoJ's concerns about the legality of the program with FBI Director Mueller on 1 March 2004. Mueller told us that this was the first time he had been made aware of DoJ's concerns.

[13] (U) Ashcroft's doctors did not clear Ashcroft to resume his duties as Attorney General until 31 March 2004.

~~(TS//SI//NF)~~ As a result of Gonzales's request, Goldsmith, Philbin, and Comey re-examined Yoo's memorandums with a view toward determining whether they adequately described the actual collection activities of the NSA under the Presidential Authorizations. They concluded that the memorandums did not. According to Goldsmith, the conclusion that Yoo's memorandums failed to accurately describe, let alone provide a legal analysis of (b) (5), (b)(1), (b)(3) meant that OLC could not tell the White House that the program could continue under the authority of those legal memorandums.

~~(TS//SI//NF)~~ On 6 March 2004, Goldsmith and Philbin, with Comey's concurrence, went to the White House to meet with Addington and Gonzales to convey their conclusions that (b) (5), (b)(1), (b)(3) According to Goldsmith's notes, Addington and Gonzales "reacted calmly and said they would get back with us." On Sunday, 7 March 2004, Goldsmith and Philbin met again with Addington and Gonzales at the White House. According to Goldsmith, the White House officials informed Goldsmith and Philbin that they disagreed with their interpretation of Yoo's memorandums and on the need to change the scope of the NSA's collection under the PSP.

~~(S//NF)~~ On 9 March 2004, Gonzales called Goldsmith to the White House in an effort to persuade him that his criticisms of Yoo's memorandums were incorrect and that Yoo's analysis provided sufficient legal support for the program. (b) (5) After Goldsmith stated that he disagreed, Gonzales next argued for a "30-day bridge" to get past the expiration of the current Presidential Authorization on 11 March 2004. Gonzales reasoned that Ashcroft, who was still hospitalized, was not in any condition to sign a renewal of the authorization, and that a "30-day bridge" would move the situation to a point where Ashcroft would be well enough to approve the program. Goldsmith told Gonzales he could not agree to recommend an extension because aspects of the program lacked legal support.

~~(TS//SI//NF)~~ At noon on 9 March, another meeting was held at the White House in Card's office. According to Mueller's notes, Mueller, Card, Vice President Cheney, Deputy Director of Central Intelligence John E. McLaughlin, Hayden, Gonzales, and other unspecified officials were present. Comey, Goldsmith, and Philbin were not invited to this meeting. After a presentation on the value of the PSP by NSA and CIA officials, it was then explained to the group that Comey "has problems" with (b)(1), (b)(3) Mueller's notes state that the Vice President suggested that "the President may have to reauthorize without [the] blessing of DoJ," to which Mueller responded, "I could have a problem with that," and that the FBI would "have to review legality of continued participation in the program."

~~(TS//SI//NF)~~ A third meeting at the White House was held on 9 March, this time with Comey, Goldsmith, and Philbin present. Gonzales told us that the meeting was held to make sure that Comey understood what was at stake with the program and to demonstrate its value. Comey said the Vice President stressed that the program was "critically

important" and warned that Comey would risk "thousands" of lives if he did not agree to recertify it. Comey said he stated at the meeting that he, as Acting Attorney General, could support reauthorizing (b)(1), (b)(3) provided the collection was (b)(1), (b)(3) However, he told the group "we can't get there" on (b)(1), (b)(3) According to Comey, the White House officials said they could not agree to that modification.

~~(S//NF)~~ Gonzales told us that after President Bush was advised of the results of the 9 March meetings, he instructed the Vice President on the morning of 10 March to call a meeting with Congressional leaders to advise them of the impasse with DoJ. That afternoon, Gonzales and other White House and IC officials, including Vice President Cheney, Card, Hayden, McLaughlin, and Tenet, convened an "emergency meeting" with Congressional leaders in the White House Situation Room. The Congressional leaders in attendance were Senate Majority and Minority Leaders William H. "Bill" Frist and Thomas A. Daschle; Senate Select Committee on Intelligence Chairman Pat Roberts and Vice Chairman John D. Rockefeller, IV; Speaker of the House J. Dennis Hastert and House Minority Leader Nancy Pelosi; and House Permanent Select Committee on Intelligence Chair Porter Goss and Ranking Member Jane Harman. No DoJ officials were asked to be present at the meeting.

~~(S//NF)~~ According to Gonzales's notes of the meeting, individual Congressional leaders expressed thoughts and concerns related to the program. Gonzales told us that the consensus was that the program should continue. Gonzales also said that following the meeting with Congressional leaders, President Bush instructed him and Card to go to the George Washington University Hospital to speak to Ashcroft, who was in the intensive care unit recovering from surgery.

(U) According to notes from Ashcroft's FBI security detail, at 18:20 on 10 March 2004, Card called the hospital and spoke with an agent in the security detail, advising the agent that President Bush would be calling shortly to speak with Ashcroft. Ashcroft's wife told the agent that Ashcroft would not accept the call. Ten minutes later, the agent called Ashcroft's Chief of Staff David Ayres at DoJ to request that Ayres speak with Card about the President's intention to call Ashcroft. The agent conveyed to Ayres Mrs. Ashcroft's desire that no calls be made to Ashcroft for another day or two. However, at 18:45, Card and the President called the hospital and, according to the agent's notes, "insisted on speaking [with Attorney General Ashcroft]." According to the agent's notes, Mrs. Ashcroft took the call from Card and the President and was informed that Gonzales and Card were coming to the hospital to see Ashcroft regarding a matter involving national security.

(U) At approximately 19:00, Ayres was advised that Gonzales and Card were on their way to the hospital. Ayres then called Comey, who at the time was being driven home by his security detail, and told Comey that Gonzales and Card were on their way to the

hospital. Comey told his driver to take him to the hospital. According to his May 2007 testimony before the Senate Judiciary Committee, Comey then called his Chief of Staff, Chuck Rosenberg, and directed him to "get as many of my people as possible to the hospital immediately." Comey next called Mueller and told him that Gonzales and Card were on their way to the hospital to see Ashcroft, and that Ashcroft was in no condition to receive visitors, much less make a decision about whether to recertify the PSP. According to Mueller's notes, Comey asked Mueller to come to the hospital to "witness [the] condition of AG." Mueller told Comey he would go to the hospital right away.

(U) Comey arrived at the hospital between 19:10 and 19:30. Comey said he began speaking to Ashcroft, and that it was not clear that Ashcroft could focus and that he "seemed pretty bad off." Goldsmith and Philbin also had been summoned to the hospital and arrived within a few minutes of each other. Comey, Goldsmith, and Philbin met briefly in an FBI "command post" that had been set up in a room adjacent to Ashcroft's room. Moments later, the command post was notified that Card and Gonzales had arrived at the hospital and were on their way upstairs to see Ashcroft. Comey, Goldsmith, and Philbin entered Ashcroft's room and, according to Goldsmith's notes, Comey and the others advised Ashcroft "not to sign anything."

(U) Gonzales and Card entered Ashcroft's hospital room at 19:35. Gonzales told us that he had with him in a manila envelope the 11 March 2004, Presidential Authorization for Ashcroft to sign. According to Philbin, Gonzales first asked Ashcroft how he was feeling. Ashcroft replied, "not well." Gonzales then said words to the effect, "You know, there's a reauthorization that has to be renewed . . .." Gonzales told us that he may also have told Ashcroft that White House officials had met with Congressional leaders "to pursue a legislative fix."

~~(TS//SI//NF)~~ Comey testified to the Senate Judiciary Committee that at this point Ashcroft told Gonzales and Card "in very strong terms" his objections to the PSP, which Comey testified Ashcroft drew from his meeting with Comey about the program a week earlier. Goldsmith's notes indicate that Ashcroft complained in particular that NSA's collection activities exceeded the scope of the authorizations and the OLC memorandums. Comey testified that Ashcroft next stated:

> "But that doesn't matter, because I'm not the Attorney General. There is the Attorney General," and he pointed to me—I was just to his left. The two men [Gonzales and Card] did not acknowledge me; they turned and walked from the room.

(U) Moments after Gonzales and Card departed, Mueller arrived at the hospital. Mueller met briefly with Ashcroft and later wrote in his notes, "AG in chair; is feeble, barely articulate, clearly stressed."

(U) Before leaving the hospital, Comey received a call from Card. Comey testified that Card was very upset and demanded that Comey come to the White House immediately. Comey told Card that he would meet with him, but not without a witness, and that he intended that witness to be Solicitor General Theodore B. Olson.

(U) Comey and the other DoJ officials left the hospital at 20:10 and met at DoJ. They were joined there by Olson. During this meeting, a call came from the Vice President for Olson, which Olson took on a secure line in Comey's office while Comey waited outside. Comey told us he believes the Vice President effectively read Olson into the program during that conversation. Comey and Olson then went to the White House at about 23:00 that evening and met with Gonzales and Card. Gonzales told us that little more was achieved at this meeting than a general acknowledgement that a "situation" continued to exist because of the disagreement between DoJ and the White House regarding the program.

~~(S//NF)~~ White House Counsel Certifies Presidential Authorization Without Department of Justice Concurrence

~~(TS//STLW//SI//OC/NF)~~ On the morning of 11 March 2004, with the Presidential Authorization set to expire, President Bush signed a new authorization for the PSP. In a departure from the past practice of having the Attorney General certify the authorization as to form and legality, the 11 March authorization was certified by White House Counsel Gonzales. The 11 March authorization also differed markedly from prior authorizations in three other respects.

~~(TS//STLW//SI//OC/NF)~~ The first significant difference between the 11 March 2004 Presidential Authorization and prior authorizations was the President's explicit assertion that the exercise of his Article II Commander-in-Chief authority "displace[s] the provisions of law, including the Foreign Intelligence Surveillance Act and chapter 119 of Title 18 of the United States Code (including 18 U.S.C. §2511(f) relating to exclusive means), to the extent of any conflict between the provisions and such exercises under Article II." Subsequent Presidential Authorizations did not include this particular language.

~~(TS//STLW//SI//OC/NF)~~ Second, to narrow the gap between the authority given on the face of prior authorizations and the actual operation of the program by the NSA, the terms governing the collection of telephony and Internet metadata were clarified. The underlying language for "acquiring" both telephony and Internet metadata remained as it had been, giving the NSA authority to "acquire" the metadata:

> when (i) at least one party to such communication is outside the United States, (ii) no party to such communication is known to be a citizen of the United States, or (iii) based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are specific and articulable facts giving reason to believe that such communication relates to international terrorism, or activities in preparation therefor. [Presidential Authorization, 11 March 2004, para. 4(b).]

However, this language was now qualified by the following two subparagraphs:

> (i) the Department of Defense may obtain and retain header/router/addressing-type information, including telecommunications dialing-type data, (b)(1), (b)(3) provided that search and retrieval from such obtained header/router/addressing-type information, including telecommunications dialing-type data, shall occur only in accordance with this authorization; and
>
> (ii) header/router/addressing-type information, including telecommunications dialing-type data, is "acquired" for purposes of subparagraph 4(b) above when, and only when, the Department of Defense has searched for and retrieved such header/router/addressing-type information, including telecommunications dialing-type data (and not when the Department obtains such header/router/addressing-type information, including telecommunications dialing-type data, such as (b)(1), (b)(3) for retention). [Id. at para. 4(b)(i) & (ii).]

~~(TS//STLW//SI//OC/NF)~~ The 11 March 2004 authorization for the first time sought to make clear that the NSA could "obtain and retain" telephony and Internet metadata in bulk (b)(1), (b)(3) but the metadata collected could only be queried ("acquired") in accordance with any of the three conditions set forth in paragraph 4(b). The language clarifying what the term "acquire" meant was included in every successive Presidential Authorization for the remainder of the program. (b)(5), (b)(1), (b)(3)

~~(TS//SI//NF)~~ The third departure from prior authorizations was the inclusion of a statement that "the Attorney General of the United States approved as to form and legality [all prior Presidential Authorizations] authorizing the same activities as are extended by this authorization." (Id. at para. 10.)[14]

~~(TS//SI//NF)~~ Card informed Comey by telephone on the morning of 11 March 2004 that the President had signed the new authorization that morning. At approximately 12:00, Gonzales called Goldsmith to inform him that the President, in issuing the authorization, had made an interpretation of law concerning his authorities and that DoJ should not act in contradiction of the President's determinations.

~~(TS//SI//NF)~~ Also at 12:00 on 11 March, Mueller met with Card at the White House. According to Mueller's notes, Card summoned Mueller to his office to bring Mueller up-to-date on the events of the preceding 24 hours, including the briefing of the Congressional leaders the prior afternoon and the President's issuance of the new authorization without DoJ's certification as to legality. In addition, Card told Mueller that if no "legislative fix" could be found by 6 May 2004, when the 11 March authorization was set to expire, the program would be discontinued.

~~(TS//SI//NF)~~ According to Mueller's notes, Card acknowledged to Mueller that President Bush had sent him and Gonzales to the hospital to seek Ashcroft's certification for the 11 March 2004 authorization, but that Ashcroft had said he was too ill to make the determination and that Comey was the Acting Attorney General. Mueller wrote that he told Card that the failure to have DoJ representation at the Congressional briefing and the attempt to have Ashcroft certify the authorization without going through Comey "gave the strong perception that the [White House] was trying to do an end run around the Acting [Attorney General] whom they knew to have serious concerns as to the legality of portions of the program." Card responded that he and Gonzales were unaware at the time of the hospital visit that Comey was the Acting Attorney General, and that they had only been following the directions of the President.

~~(S//NF)~~ Several senior DoJ and FBI officials, including Comey, Goldsmith, and Mueller considered resigning after the 11 March 2004 Presidential Authorization was signed without DoJ's concurrence. These officials cited as reasons for considering resignation the manner in which the White House had handled its dispute with DoJ and the treatment of Ashcroft, among other reasons.

~~(S//NF)~~ On 12 March 2004, Mueller drafted by hand a letter stating, in part: "[A]fter reviewing the plain language of the FISA statute, and the order issued yesterday by the President . . . and in the absence of further clarification of the legality of the program from the Attorney General, I am forced to withdraw the FBI from participation in the program.

---

[14] (b) (5)

Further, should the President order the continuation of the FBI's participation in the program, and in the absence of further legal advice from the AG, I would be constrained to resign as Director of the FBI." Mueller told us he planned on having the letter typed and then tendering it, but that based on subsequent events his resignation was not necessary.

~~(TS//SI//NF)~~ Mueller sent Comey a memorandum seeking guidance on how the FBI should proceed in light of developments related to the Presidential Authorizations. The memorandum asked whether FBI agents detailed to the NSA to work on the PSP should be recalled; whether the FBI should continue to receive and investigate tips based on [redacted] (b)(1), (b)(3) and whether (b)(1), (b)(3) [redacted] b1, b3, b7E

(U) On the morning of 12 March, Comey and Mueller attended the regular daily threat briefing with the President in the Oval Office. Comey said that, following the briefing, President Bush called him into the President's private study for an "unscheduled meeting." Comey told the President of DoJ's legal concerns regarding the PSP. According to Comey, the President's response indicated that he had not been fully informed of these concerns. Comey told the President that the President's staff had been advised of these issues "for weeks." According to Comey, the President said that he just needed until May 6 (the date of the next authorization), and that if he could not get Congress to fix FISA by then he would shut down the program. The President emphasized the importance of the program and that it "saves lives."

~~(TS//SI//NF)~~ The President next met with Mueller. According to Mueller's notes, Mueller told the President of his concerns regarding the FBI's continued participation in the program without an opinion from the Attorney General as to its legality, and that he was considering resigning if the FBI were directed to continue to participate without the concurrence of the Attorney General. The President directed Mueller to meet with Comey and other PSP principals to address the legal concerns so that the FBI could continue participating in the program "as appropriate under the law." Comey decided not to direct the FBI to cease cooperating with the NSA in conjunction with the PSP. Comey's decision is documented in a one-page memorandum from Goldsmith to Comey in which Goldsmith explained that the President, as Commander-in-Chief and Chief Executive with the constitutional duty to "take care that the laws are faithfully executed," made a determination that the PSP, as practiced, was lawful. Goldsmith concluded that this determination was binding on the entire Executive Branch, including Comey in his exercise of the powers of the Attorney General.

~~(TS//SI//NF)~~ The same day, an interagency working group was convened to continue reanalyzing the legality of the PSP. In accordance with the President's directive to Mueller, officials from the FBI, NSA, and CIA were brought into the process, although the OLC maintained the lead role. On 16 March 2004, Comey drafted a memorandum to Gonzales setting out Comey's advice to the President regarding the PSP. Comey advised that the President may lawfully continue (b)(1), (b)(3) [redacted] Comey further

wrote that DoJ remained unable to find a legal basis to support (b)(1), (b)(3) and he advised that such (b)(1), (b)(3) Finally, Comey cautioned that he believed the ongoing collection of (b)(1), (b)(3) raised "serious issues" about Congressional notification, "particularly where the legal basis for the program is the President's decision to assert his authority to override an otherwise applicable Act of Congress."

(U) Gonzales replied by letter on the evening of 16 March. The letter stated, in part:

> Your memorandum appears to have been based on a misunderstanding of the President's expectations regarding the conduct of the Department of Justice. While the President was, and remains, interested in any thoughts the Department of Justice may have on alternative ways to achieve effectively the goals of the activities authorized by the Presidential Authorization of March 11, 2004, the President has addressed definitively for the Executive Branch in the Presidential Authorization the interpretation of the law.

~~(TS//SI//NF)~~ White House Agrees to (b)(1), (b)(3)

~~(TS//SI//NF)~~ Notwithstanding Gonzales's letter, on 17 March 2004 the President decided to (b)(1), (b)(3) The President's directive was expressed in two modifications to the 11 March 2004 Presidential Authorization.

~~(TS//STLW//SI//OC/NF)~~ On 19 March 2004, the President signed, and Gonzales certified as to form and legality, a modification of the 11 March 2004 Presidential Authorization. The modification made two significant changes to the current authorization and a third important change affecting all subsequent authorizations. First, the modification (b)(1), (b)(3) Second, the modification (b)(1), (b)(3)

[redacted] Third, the modification authorized
(b)(1), (b)(3)
[redacted]

~~(TS//STLW//SI//OC/NF)~~ On 2 April 2004, President Bush signed, and Gonzales certified as to form and legality, a second modification of the 11 March 2004, Presidential Authorization. This modification addressed only [redacted] of the PSP.
(b)(1), (b)(3)
[redacted]

~~(S//NF)~~ On 6 May 2004, Goldsmith and Philbin completed an OLC legal memorandum assessing the legality of the PSP as it was then operating. The memorandum stated that the AUMF passed by Congress shortly after the attacks of 11 September 2001 gave the President authority to use both domestically and abroad "all necessary and appropriate force," including SIGINT capabilities, to prevent future acts of international terrorism against the United States. According to the memorandum, the AUMF was properly read as an express authorization to conduct targeted electronic surveillance against al-Qa'ida and its affiliates, the entities responsible for attacking the United States, thereby supporting the President's directives to conduct these activities under the PSP. Much of the legal reasoning in the 6 May 2004 OLC memorandum was publicly released by DoJ in a "White Paper"—"Legal Authorities Supporting the Activities of the National Security Agency Described by the President"—issued on 19 January 2006 after the content

---

(b) (5), (b)(1), (b)(3)
(b)(1), (b)(3)
[redacted]

collection portion of the program was revealed in *The New York Times* and publicly confirmed by the President in December 2005.

(U) Restrictions on Access to the President's Surveillance Program Impeded Department of Justice Legal Review

~~(TS//SI//OC/NF)~~ The DoJ IG found it extraordinary and inappropriate that a single DoJ attorney, John Yoo, was relied upon to conduct the initial legal assessment of the PSP, and that the lack of oversight and review of Yoo's work, which was contrary to the customary practice of OLC, contributed to a legal analysis of the PSP that, at a minimum, was factually flawed. Deficiencies in the legal memorandums became apparent once additional DoJ attorneys were read into the program in 2003 and those attorneys sought a greater understanding of the PSP's operation. The White House's strict controls over access to the PSP undermined DoJ's ability to provide the President the best available advice about the program. The DoJ IG also concluded that the circumstances plainly called for additional DoJ resources to be applied to the legal review of the program, and that it was the Attorney General's responsibility to be aware of this need and to take steps to address it. However, the DoJ OIG could not determine whether Ashcroft aggressively sought additional read-ins to assist with DoJ's legal review of the program prior to 2003 because Ashcroft did not agree to be interviewed.

(U) TRANSITION OF PRESIDENT'S SURVEILLANCE PROGRAM ACTIVITIES TO FOREIGN INTELLIGENCE SURVEILLANCE ACT AUTHORITY

~~(TS//SI//NF)~~ Internet Metadata Collection Transition to Operation Under FISA Authority

~~(TS//SI//OC/NF)~~ [redacted] (b)(1), (b)(3)

~~(TS//SI//NF)~~ The government's FISA application, entitled "Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes," was filed [redacted] (b)(1), (b)(3) The application package included:

- A proposed order authorizing the collection activity and secondary orders mandating carriers to cooperate.
- A declaration by Hayden explaining the technical aspects of the proposed Internet metadata collection and identifying the government official

seeking to use the pen register and trap and trace (PR/TT) devices covered by the application for purposes of 50 U.S.C. § 1842(c)(1).

- A declaration by Tenet describing the threat posed by (b)(1), (b)(3) to the United States.
- A certification from Ashcroft stating that the information likely to be obtained from the PR/TT devices was relevant to an ongoing investigation to protect against international terrorism, as required by 50 U.S.C. § 1842(c).
- A memorandum of law and fact in support of the application.

(~~TS//SI//OC/NF~~) The objective of the application was to secure authority under FISA to collect (b)(1), (b)(3) bulk Internet metadata (b)(1), (b)(3) DoJ constructed its legal argument for this novel use of PR/TT devices around traditional authorities provided under FISA. (See 50 U.S.C. § 1842(a)(1).) The government argued that the NSA's proposed collection of metadata met the requirements of FISA by noting that the metadata sought comported with the "dialing, routing, addressing, or signaling information" type of data described in FISA's definitions of PR/TT devices. (See 18 U.S.C. § 3127(3) and (4).) The government next argued that the information likely to be obtained from the PR/TT devices was relevant to an ongoing investigation to protect against international terrorism, as certified by the Attorney General under 50 U.S.C. § 1842(c). In support of this "certification of relevance" the government stated that the FBI The government also stated that the NSA needed to collect metadata in bulk to effectively perform contact chaining (b)(1), (b)(3) that would enable the NSA to discover enemy communications. b1, b3, b7E

(~~TS//SI//NF~~) The application requested that the NSA be authorized to collect metadata (b)(1), (b)(3) The application represented that for most of the proposed collection on it was "overwhelmingly likely" that at least one end of the transmitted communication either originated in or was destined for locations outside the United States, and that in some cases both ends of the communication were entirely foreign. However, the government acknowledged that (b)(1), (b)(3)

(b)(1), (b)(3)

(~~TS//SI//NF~~) The application proposed allowing 10 NSA analysts access to the database. The NSA analysts were to be briefed by NSA OGC personnel concerning the circumstances under which the database could be queried, and all queries would have to be

approved by one of seven senior NSA officials. The application proposed that queries of the Internet metadata archive would be performed when the Internet communication address met the following standard:

> [B]ased on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known e-mail address is associated with (b)(1), (b)(3) [redacted]

~~(TS//SI//OC/NF)~~ The application and supporting documents explained that the NSA intended to use the Internet metadata to develop contact chaining (b)(1), (b)(3) [redacted] The NSA estimated that its queries of the database would generate approximately 400 tips to the FBI and CIA each year. Of these tips, the NSA projected that 25 percent would include U.S. person information, amounting to leads including information on about "four to five U.S. persons each month."

~~(TS//SI//NF)~~ On 14 July 2004, Kollar-Kotelly signed a Pen Register and Trap and Trace Opinion and Order (PR/TT Order) based on her findings that the proposed collection of Internet metadata and the government's proposed controls over and dissemination of this information satisfied the requirements of FISA. The PR/TT Order, which granted the government's application in all key respects, approved for a period of 90 days the collection within the United States of Internet metadata (b)(1), (b)(3) [redacted]

~~(TS//SI//NF)~~ The PR/TT Order also required the government to comply with certain additional restrictions and procedures either adapted from or not originally proposed in the application. The FISC amended the government's proposed querying standard, consistent with 50 U.S.C. § 1842(c)(2), to include the proviso that the NSA may query the database based on its reasonable articulable suspicion that a particular known Internet communication address is associated with (b)(1), (b)(3) [redacted] "provided, however, that an (b)(1), (b)(3) [redacted] believed to be used by a U.S. person shall not be regarded as associated with (b)(1), (b)(3) [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution." Regarding the storing, accessing, and disseminating of the Internet metadata obtained by the NSA, the FISC ordered that the NSA store the information in a manner that ensures it is not commingled with other data, and "generate a log of auditing information for each occasion when the information is accessed, to include the ... retrieval request." The FISC also issued separate orders to (b)(1), (b)(3) [redacted] service providers (b)(1), (b)(3) [redacted] to assist the NSA with the installation and use of the PR/TT devices and to maintain the secrecy of the NSA's activities.

b1, b3, b7E

~~(TS//SI//NF)~~ Several officials told us that obtaining the PR/TT Order was seen as a great success, and that there was general agreement that the government had secured all the authority it sought to conduct the bulk Internet metadata collection.

~~(TS//SI//NF)~~ The FISC first renewed the PR/TT Order on (b)(1), (b)(3) and then renewed it by subsequent orders at approximately 90-day intervals. In these renewals, the FISC (b)(1), (b)(3) that it approved with the 14 July 2004 PR/TT Order. Under the PR/TT renewal applications, the scope of authorized queries against the PR/TT database remained limited to queries that concerned (b)(1), (b)(3) b1, b3, b7E

[redacted]

(U) Department of Justice Notices of Compliance Incidents

~~(TS//SI//NF)~~ On (b)(1), (b)(3) DoJ OIPR filed a Notice of Compliance Incidents with the FISC describing certain "unauthorized collection" that had taken place following issuance of the PR/TT Order. (b)(1), (b)(3)

[redacted]

~~(TS//SI//NF)~~ On (b)(1), (b)(3) the FISC issued a Compliance Order stating that the "NSA violated its own proposed limitations." The FISC stated that it was troubled by the duration of the violations, which extended from 14 July through (b)(1), (b)(3) and that the Court was reluctant to issue a renewal of the PR/TT Order as to (b)(1), (b)(3) However, Kollar-Kotelly signed a Renewal Order on (b)(1), (b)(3) allowing the NSA to continue collecting Internet metadata under FISA on terms similar to the original PR/TT Order. (b)(1), (b)(3)

[redacted]

(b)(3)

[redacted]

~~(TS//SI//NF)~~ **Telephony Metadata Collection Transition to Operation Under FISA Authority**

~~(TS//SI//NF)~~ Another part of the PSP, bulk collection of telephony metadata, was brought under FISA authority in May 2006. As with Internet metadata, the bulk nature of the telephony metadata collection provided the NSA the ability to conduct contact chaining (b)(1), (b)(3) [redacted]

~~(TS//SI//NF)~~ The transition of bulk telephony metadata collection from Presidential authority to FISA authority relied on a provision in FISA that authorized the FBI to seek an order from the FISC compelling the production of "any tangible things" from any business, organization, or entity, provided the items are for an authorized investigation to protect against international terrorism or clandestine intelligence activities. (See 50 U.S.C. § 1861.) Orders under this provision are commonly referred to as "Section 215" orders in reference to Section 215 of the USA PATRIOT Act, which amended the "business records" provision in Title V of FISA.[18] The "tangible things" sought in this Section 215 application were the telephone call detail records of certain telecommunications service providers.

~~(TS//SI//NF)~~ The timing of the decision in May 2006 to seek a FISC order for the bulk collection of telephony metadata was driven primarily by external events. A 16 December 2005 article in *The New York Times* entitled, "Bush Lets U.S. Spy on Callers Without Courts," described in broad terms the content collection aspect of the PSP. (b)(1), (b)(3) [redacted] On 17 December 2005, in response to the article, President Bush publicly confirmed that he had authorized the NSA to intercept the international communications of people with known links to al-Qa'ida and related terrorist organizations. On 19 January 2006, DoJ issued its White Paper—"Legal Authorities Supporting the Activities of the National Security Agency Described by the President"—that addressed in an unclassified form the legal basis for the collection activities described in *The New York Times* article and confirmed by the President.

[18] (U) Prior to the enactment of Section 215 of the USA PATRIOT Act, the FISA "business records" provisions were limited to obtaining information about a specific person or entity under investigation and only from common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities.

~~(TS//SI//NF)~~ According to Bradbury, the head of OLC at that time, the legal analysis contained in the White Paper (b)(1), (b)(3) Although *The New York Times* article did not describe this aspect of the PSP, reporters at *USA Today* asked about this aspect of the program in early 2006. Bradbury (b)(1), (b)(3) anticipated that a *USA Today* article would attract significant public attention when published. As anticipated, on 11 May 2006, the *USA Today* published the results of its investigation in an article entitled, "NSA Has Massive Database of American Phone Calls."

~~(TS//SI//NF)~~ On 23 May 2006, the FBI filed with the FISC a Section 215 application seeking authority to collect telephony metadata to assist the NSA in finding and identifying members or agents of (b)(1), (b)(3) in support of the (b)(1), (b)(3) FBI investigations then pending and other IC operations. The application requested an order compelling certain telecommunications companies to produce (for the duration of the 90-day order) call detail records relating to all telephone communications maintained by the carriers. According to the application, the majority of the telephony metadata provided to the NSA was expected to involve communications that were (1) between domestic and foreign locations, or (2) wholly within the United States, including local telephone calls. The application estimated that the collection would involve the NSA receiving approximately (b)(1), (b) call detail records per day.[19] b1, b3, b7E

~~(TS//SI//NF)~~ The application acknowledged that the vast collection would include communications records of U.S. persons located within the United States who were not the subject of any FBI investigation. However, relying on the precedent established by the PR/TT Order, the application asserted that the collection was needed for the NSA to find (b)(1), (b)(3) and to identify unknown operatives, some of whom may be in the United States or in communication with U.S. persons, by using contact chaining (b)(1), (b)(3) As was done under the PSP, the call detail records would be entered in an NSA database and analysts would query the data with particular telephone numbers to identify connections with other numbers (b)(1), (b)(3) The proposed query standard in the Section 215 application essentially was the same standard applied under the PSP in connection with telephony metadata, and the same standard the FISC authorized in the PR/TT Order for Internet metadata. The Section 215 application also included in the proposed query standard the First Amendment proviso that the FISC added to the PR/TT query standard. b1, b3, b7E

[19] ~~(TS//SI//NF)~~ The actual average amount of telephony metadata collected per day (b)(1), (b) (3) call detail records rather than (b)(1), (b) estimated in the application.

~~(TS//SI//NF)~~ On 24 May 2006, the FISC approved the Section 215 application, finding that there were reasonable grounds to believe that the telephony metadata records sought were relevant to authorized investigations the FBI was conducting to protect against international terrorism. The FISC Section 215 order incorporated each of the procedures proposed in the government's application relating to access to and use of the metadata, which were nearly identical to those included in the Internet metadata PR/TT Order.

~~(TS//SI//NF)~~ Through March 2009, the FISC renewed the authorities granted in the 24 May 2006 order at approximately 90-day intervals, with some modifications sought by the U.S. government. For example, the FISC granted an August 2006 motion requesting (b)(1), (b)(3) Except for these and other minor modifications, the terms of the FISC's grant of Section 215 authority for the bulk collection of telephony metadata remained essentially unchanged from the first approval in May 2006 until March 2009. (b)(1), (b)(3) Further, the FISC's Section 215 Orders did not require the NSA to modify its use of the telephony metadata from an analytical perspective. NSA analysts were authorized to query the data as they had under the PSP, conduct metadata analysis, and disseminate the results to the FBI, the CIA, and other customers.

~~(TS//SI//NF)~~ However, the FISC drastically changed the authority contained in its March 2009 Section 215 Order after it was notified in January 2009 that the NSA had been querying the metadata in a manner that was not authorized by the court's Section 215 Orders. Specifically, the NSA, on a daily basis, was automatically querying the metadata with (b)(1), (b)(3) telephone numbers from an alert list that had not been determined to satisfy the reasonable articulable suspicion standard required by the FISC to access the telephony metadata for search or analysis purposes.

~~(TS//SI//NF)~~ On 2 March 2009, the FISC issued an order that addressed the compliance incidents that had been reported in January 2009, the government's explanation for their occurrence, and the remedial and prospective measures being taken in response. The FISC stated its concerns with the telephony metadata program and its lack of confidence "that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders." Nonetheless, the FISC authorized the government to continue collecting telephony metadata under the Section 215 Orders. The FISC explained that in light of the government's repeated representations that the collection of the telephony metadata is vital to national security, taken together with the court's prior determination that the collection properly administered conforms with the FISA statute, that "it would not be prudent" to order the government to cease the bulk collection.

~~(TS//SI//NF)~~ However, believing that "more is needed to protect the privacy of U.S. person information acquired and retained" pursuant to the Section 215 Orders, the FISC prohibited the government from accessing the metadata collected "until such time as the government is able to restore the Court's confidence that the government can and will comply with previously approved procedures for accessing such data." The government may, on a case-by-case basis, request authority from the FISC to query the metadata with a specific telephone number to obtain foreign intelligence. The FISC also authorized the government to query the metadata without court approval to protect against an imminent threat to human life, provided the government notifies the court within the next business day.

~~(TS//SI//NF)~~ Content Collection Transition to Operation Under FISA Authority

~~(TS//SI//NF)~~ The last part of the PSP brought under FISA authority was telephone and Internet communications content collection. As explained below, the effort to accomplish this transition was legally and operationally complex and required an enormous effort on the part of the government and the FISC. The FISC judge who ruled on the initial application approved the unconventional legal approach the government proposed to fit PSP's content collection activities within FISA. However, the FISC judge responsible for considering the government's renewal application rejected the legal approach. This resulted in significant diminution in authorized surveillance activity involving content collection and hastened the enactment of legislation that significantly amended FISA and provided the government surveillance authorities broader than those authorized under the PSP.

[redacted]

~~(TS//SI//NF)~~ The government filed the content collection application with the FISC on 13 December 2006. The application sought authority to intercept the content of telephone and electronic communications of [redacted] The application sought to replace the conventional practice under FISA of filing individual applications each time the government had probable cause to believe that a particular telephone number or Internet communication address was being used or about to be used by members or agents of a foreign power. In the place of the individualized process, the application proposed that the FISC establish broad parameters for the interception of communications—the groups that can be targeted and the locations where the surveillance can be conducted—and that NSA officials, rather than FISC judges, determine within these parameters the particular selectors to be collected against. [redacted]

[redacted] albeit with FISC review and supervision. The government's approach in the FISA application rested on a broad interpretation of the statutory term "facility" and the use of minimization procedures by NSA officials to make probable cause determinations about individual selectors, rather than have a FISC judge make such determinations.

~~(TS//SI//NF)~~ In short, the government's content application asked the FISC to find probable cause to believe that [redacted] engaged in international terrorism, and that [redacted] Then, within these parameters, NSA officials would make probable cause findings (subsequently reviewed by the FISC) about whether individual telephone numbers or Internet communications addresses are used by members or agents of [redacted] and whether the communications of those numbers and addresses are to or from a foreign country. When probable cause findings were made, the NSA could direct the telecommunications companies to provide the content of communications associated with those telephone numbers and Internet communications addresses.

~~(TS//STLW//SI//OC/NF)~~ On 10 January 2007, Judge Malcolm J. Howard approved the government's 13 December 2006 content application as it pertained to foreign selectors—telephone numbers and Internet communications addresses reasonably believed to be used by individuals outside the United States. The effort to implement the order was a massive undertaking for DoJ and NSA. At the time of the order, the NSA was actively tasking for content collection approximately [redacted] foreign selectors—Internet communications addresses or telephone numbers—under authority of the PSP. Approximately [redacted] of these were filed with Howard on an approved schedule of rolling submissions over the 90-day duration of the order.

~~(TS//SI//NF)~~ However, Howard did not approve the government's 13 December 2006 content application as it pertained to domestic selectors—telephone numbers and Internet communications addresses reasonably believed to be used by individuals in the United States. Howard advised DoJ to file a separate application for the international calls of domestic selectors that took a more traditional approach to FISA. A more traditional approach meant that the facilities targeted by the FISA application should be particular telephone numbers and Internet communication addresses and that the probable cause determination for a particular selector would reside with the FISC. DoJ did this in an application filed on 9 January 2007, which Howard approved the following day. The FISC renewed the domestic selectors order approved by Howard for the final time in [redacted] and it has since expired.

~~(TS//SI//NF)~~ DoJ's first renewal application to extend the foreign selectors authorities was filed on 20 March 2007 with Judge Roger Vinson, the FISC duty judge that week. On 29 March 2007, Vinson orally advised DoJ that he could not approve the application and, on 3 April 2007, he issued an order and Memorandum Opinion explaining the reasoning for his conclusion. Vinson wrote that DoJ's foreign selectors renewal application concerns an "extremely important issue" regarding who may make probable cause findings that determine the individuals and the communications that can be subjected to electronic surveillance under FISA. In Vinson's view, the question was whether probable cause determinations are required to be made by the FISC through procedures established by statute, or whether the NSA may make such determinations under an alternative mechanism cast as "minimization procedures." Vinson concluded, based on past practice under FISA and the Congressional intent underlying the statute, that probable cause determinations must be made by the FISC.

~~(TS//SI//NF)~~ Vinson also wrote that he was mindful of the government's argument that the government's proposed approach to foreign selectors was necessary to provide or enhance the "speed and flexibility" with which the NSA responds to threats, and that foreign intelligence information may be lost in the time it takes to obtain Attorney General emergency authorizations. However, in Vinson's view, FISA's requirements reflected a balance struck by Congress between privacy interests and the need to obtain foreign intelligence information, and until Congress took legislative action on FISA to respond to the government's concerns, the FISC must apply the statute's procedures. He concluded that the government's application sought to strike a different balance for the surveillance of foreign telephone numbers and Internet communications addresses. Vinson rejected this position, stating, "the [FISA] statute applies the same requirements to surveillance of facilities used overseas as it does to surveillance of facilities used in the United States." Vinson suggested that, "Congress should also consider clarifying or modifying the scope of FISA and of this Court's jurisdiction with regard to such facilities . . .." Vinson's suggestion was a spur to Congress to consider FISA modernization legislation in the summer of 2007.

~~(TS//STLW//SI//OC/NF)~~ In May 2007, DoJ filed, and Vinson approved, a revised foreign selectors application that took a more traditional approach to FISA. Although the revised approach sought to preserve some of the "speed and agility" the government had under Howard's order, the comparatively laborious process for targeting foreign selectors under Vinson's order caused the government to place only a fraction of the desired foreign selectors under coverage. The number of foreign selectors on collection dropped from abou[redacted] under the January 2007 order to abou[redacted] under the May 2007 order. The situation accelerated the government's efforts to obtain legislation that would amend FISA to address the government's surveillance capabilities within the United States directed at persons located outside the United States. The Protect America Act, signed into law on 5 August 2007, accomplished this objective by authorizing the NSA to intercept inside the United States any communications of non-U.S. persons reasonably believed to be located outside the United States, provided a significant purpose of the acquisition pertains to foreign intelligence. The Protect America Act effectively superseded Vinson's foreign

selectors order and the government therefore did not seek to renew the order when it expired on 24 August 2007.

~~(TS//SI//NF)~~ The DOJ IG concluded that several considerations favored initiating PSP's transition from Presidential authority to FISA authority earlier than March 2004, especially as the program became less a temporary response to the September 11 terrorist attacks and more a permanent surveillance tool. These considerations included PSP's substantial effect on privacy interests of U.S. persons, the instability of the legal reasoning on which the program rested for several years, and the substantial restrictions placed on FBI agents' and analysts' access to and use of program-derived information due to the highly classified status of the PSP. The DOJ IG also recommended that DoJ carefully monitor the collection, use, and retention of the information that is now collected under FISA authority and, together with other agencies, continue to examine its value to the government's ongoing counterterrorism efforts.

(U) IMPACT OF THE PRESIDENT'S SURVEILLANCE PROGRAM ON INTELLIGENCE COMMUNITY COUNTERTERRORISM EFFORTS

(U) Senior Intelligence Community Officials Believe That the President's Surveillance Program Filled an Intelligence Gap

~~(TS//SI//NF)~~ Hayden, Goss, McLaughlin, and other senior IC officials we interviewed told us that the PSP addressed a gap in intelligence collection. The IC needed increased access to international communications that transited domestic U.S. communication wires, particularly international communications that originated or terminated within the United States. However, collection of such communications required authorization under FISA, and there was widespread belief among senior IC officials that the process for obtaining FISA authorization was too cumbersome and time consuming to address the current threat. [redacted] During the May 2006 Senate hearing on his nomination to be Director of the CIA, Hayden said that, had PSP been in place before the September 2001 attacks, hijackers Khalid Almihdhar and Nawaf Alhazmi almost certainly would have been identified and located.

~~(TS//SI//OC/NF)~~ According to senior NSA officials, the PSP gave NSA the capability to exploit a key terrorist vulnerability. [redacted] With PSP authority, NSA could collect communications between terrorists in the United States and members of al-Qa'ida [redacted] located in foreign countries. The PSP provided SIGINT coverage at the seam between foreign and

domestic intelligence collection. Hayden cited as an important consequence of the PSP the NSA's ability to collect more [redacted]

~~(S//NF)~~ Hayden told us that he always felt the PSP was worthwhile and successful. His expectation was that the CIA and the FBI would be customers of program-derived information and integrate it into their respective operations. [redacted] Hayden told us that the program helped to determine that terrorist cells were not embedded within the United States to the extent that had been feared.

(U) Difficulty in Assessing the Impact of the President's Surveillance Program

~~(S//SI//NF)~~ It was difficult to assess the overall impact of PSP on IC counterterrorism efforts. Except for the FBI, IC organizations that participated in the PSP did not have systematic processes for tracking how PSP reporting was used. [redacted] We were repeatedly told that the PSP was one of a number of intelligence sources and analytic tools that were available to IC personnel, and that, because PSP reporting was used in conjunction with reporting from other intelligence sources, it was difficult to attribute the success of particular counterterrorism operations exclusively to the PSP.

(U) Impact of the President's Surveillance Program on FBI Counterterrorism Efforts

~~(S//NF)~~ The DoJ IG found it difficult to assess or quantify the impact of the PSP on FBI counterterrorism efforts. However, based on our interviews of FBI managers and agents and our review of documents, we concluded that, although PSP information had value in some counterterrorism investigations, the program generally played a limited role in the FBI's overall counterterrorism efforts. Several officials we interviewed suggested that the program provided an "early warning system" to allow the IC to detect potential

terrorist attacks, even if the program had not specifically uncovered evidence of preparations for such attacks.

(U) FBI Efforts to Assess the Value of the Program

~~(TS//SI//NF)~~ The FBI made several attempts to assess the value of the PSP to FBI counterterrorism efforts. In 2004 and again in 2006, FBI's Office of General Counsel (OGC) attempted to assess the value to the FBI of PSP information. This first assessment relied on anecdotal information and informal feedback from FBI field offices. The 2006 assessment was limited to the aspect of the PSP disclosed in *The New York Times* article and subsequently confirmed by the President, i.e., content collection.

~~(S//NF)~~ The FBI undertook two more efforts to study PSP's impact on FBI operations in early 2006. In both of these statistical studies, the FBI sought to determine what percentage of PSP tippers resulted in "significant contribution[s] to the identification of terrorist subjects or activity on U.S. soil." The FBI considered a tipper significant if it led to any of three investigative results: the identification of a terrorist, the deportation from the United States of a suspected terrorist, or the development of an asset that can report about the activities of terrorists.

~~(TS//SI//OC/NF)~~ The first study examined a sample of leads selected from the [redacted] tippers the NSA provided the FBI from approximately October 2001 to December 2005. The study found that 1.2 percent of the leads made significant contributions, as defined above. The study extrapolated this figure to the entire population of leads and determined that one could expect to find that [redacted] leads made significant contributions to FBI counterterrorism efforts. The second study, which reviewed all of the [redacted] leads the NSA provided the FBI from August 2004 through January 2006, identified no instances of significant contributions to FBI counterterrorism efforts. The studies did not include explicit conclusions on the program's usefulness. However, based in part on the results of the first study, FBI executive management, including Mueller and Deputy Director John Pistole, concluded that the PSP was "of value." b1, b3, b7E

(U) FBI Judgmental Assessments of the Program

~~(S//NF)~~ We interviewed FBI headquarters and field office personnel who regularly handled PSP information for their assessments of the impact of program information on FBI counterterrorism efforts. The FBI personnel we interviewed were generally supportive of the PSP as "one tool of many" in the FBI's anti-terrorism efforts that "could help move cases forward". Even though most leads were determined not to have any connection to terrorism, many of the FBI officials believed the mere possibility of a terrorist connection made investigating the tips worthwhile.

~~(S//NF)~~ However, the exceptionally compartmented nature of the program created some frustration for FBI personnel. Some agents criticized PSP reports for providing insufficient details about the foreign individuals allegedly involved in terrorism. Others occasionally were frustrated by the prohibition on using [redacted] information in judicial processes, such as in FISA applications, although none of the FBI field office agents we interviewed could identify an investigation in which the restrictions adversely affected the case. Agents who managed counterterrorism programs at the FBI field offices we visited were critical of the [redacted] project for failing to adequately prioritize threat information and, because of the program's special status, for limiting the managers' ability to prioritize the leads in the manner they felt was warranted by the information. b1, b3, b7E

~~(S//NF)~~ Mueller told us that the PSP was useful. He said the FBI must follow every lead it receives in order to prevent future terrorist attacks and that to the extent such information can be gathered and used legally it must be exploited. He stated that he "would not dismiss the potency of a program based on the percentage of hits." Mueller added that, as a general matter, it is very difficult to quantify the effectiveness of an intelligence program without "tagging" the leads that are produced in order to evaluate the role the program information played in any investigation.

(U) Impact of the President's Surveillance Program on CIA Counterterrorism Operations

(U) The CIA Did Not Systematically Assess the Effectiveness of the Program

~~(S//NF)~~ The CIA did not implement procedures to systematically assess the usefulness of the product of the PSP and did not routinely document whether particular PSP reporting had contributed to successful counterterrorism operations. CIA officials, including Hayden, told us that PSP reporting was used in conjunction with reporting from other intelligence sources; consequently, it is difficult to attribute the success of particular counterterrorism operations exclusively to the PSP. In a May 2006 briefing to the SSCI, the Deputy Director, [redacted] said that PSP reporting was rarely the sole basis for an intelligence success, but that it frequently played a supporting role. He went on to state that the program was an additional resource to enhance the CIA's understanding of terrorist networks and to help identify potential threats to the homeland. Other [redacted] officials we interviewed said that the PSP was one of many tools available to them, and that the tools were often used in combination.

~~(S//NF)~~ [redacted] However, because there is no means to comprehensively track how PSP information was used, CIA officials were able to provide

only limited information on how program reporting contributed to successful operations, and the CIA IG was unable to independently draw any conclusion on the overall usefulness of the program to CIA.

[redacted]

(U) Several Factors Hindered CIA Utilization of the Program

~~(S//NF)~~ The CIA IG concluded that several factors hindered the CIA in making full use of the capabilities of the PSP. Many CIA officials told us that too few CIA personnel at the working level were read into the PSP. At the program's inception, a disproportionate number of the CIA personnel who were read into the PSP were senior CIA managers. [redacted] the disparity between the number of senior CIA managers read into PSP and the number of working-level CIA personnel read into the program resulted in too few CIA personnel to fully utilize PSP information for targeting and analysis.

~~(S//NF)~~ [redacted] working-level CIA analysts and targeting officers who were read into the PSP had too many competing priorities, and too many other information sources and analytic tools available to them, to fully utilize PSP. [redacted] officials also told us that much of the PSP reporting was vague or without context, which led analysts and targeting officers to rely more heavily on other information sources and analytic tools, which were more easily accessed and timely than the PSP.

~~(S//NF)~~ CIA officers said that the PSP would have been more fully utilized if analysts and targeting officers had obtained a better understanding of the program's capabilities. There was no formal training on the use of the PSP beyond the initial read in to the program. Many CIA officers we interviewed said that the instruction provided in the read-in briefing was not sufficient and that they were surprised and frustrated by the lack of additional guidance. Some officers told us that there was insufficient legal guidance on the use of PSP-derived information.

~~(S//NF)~~ The factors that hindered the CIA in making full use of the PSP might have been mitigated if the CIA had designated an individual at an appropriate level of managerial authority, who possessed knowledge of both the PSP and CIA counterterrorism activities, to be responsible and accountable for overseeing CIA participation in the

program.

[redacted]

(U) Impact of the President's Surveillance Program on NCTC Counterterrorism Efforts

(b)(1), (b)(3)

~~(S//NF)~~ [redacted] NCTC analysts characterized the PSP as a useful tool, but they also noted that the program was only one of several valuable sources of information available to them. In their view, PSP-derived information was not of greater value than other sources of intelligence. Although NCTC analysts we interviewed could not recall specific examples where PSP information provided what they considered actionable intelligence, they told us they remember attending meetings where the benefits of the PSP were regularly discussed.

(U) Counterterrorism Operations Supported by the President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ Our efforts to independently identify how PSP information impacted terrorism investigations and counterterrorism operations were hampered by the nature of these activities, which as previously stated, frequently are predicated on multiple sources of information. Many IC officials we interviewed had difficulty citing specific instances where PSP reporting contributed to a counterterrorism success. The same handful of cases tended to be cited as PSP successes by personnel we interviewed from each of the participating IC organizations and in reports, briefing charts, and other documents we reviewed. b1, b3, b6, b7C, b7E

(b)(1), (b)(3)

[redacted] These cases, and others identified to us as PSP successes, are discussed below.

~~(TS//STLW//SI//OC/NF)~~ Among the more significant PSP successes was [redacted]

b1, b3, b6, b7C, b7E

~~(TS//STLW//SI//OC/NF)~~ In [redacted] the FBI arrested [redacted] and [redacted] later pled guilty to [redacted] After [redacted] arrest, [redacted] provided valuable information to the law enforcement and intelligence communities. [redacted]

b1, b3, b6, b7C, b7E

[redacted] NSA Director Alexander cited reporting on [redacted] as the most significant success of the PSP. Alexander said that PSP reporting on [redacted] "probably saved more lives" than any other PSP information produced by NSA.

~~(TS//STLW//SI//OC/NF)~~ An [redacted] tipper, dated [redacted] reported that [redacted] Additional [redacted] reporting, in [redacted] provided telephone contacts between and among [redacted] and several individuals with suspected terrorist ties located in [redacted] The FBI learned more about [redacted] ties to terrorist groups from evidence seized [redacted] evidence gathered through several interviews [redacted] The FBI arrested [redacted] on [redacted] and [redacted] was indicted on [redacted] was convicted on [redacted] on [redacted] and was sentenced to [redacted] prison term. [redacted]

b1, b3, b6, b7C, b7E

- ~~(TS//STLW//SI//OC/NF)~~ In an undated summary of PSP successes, the NSA characterized [redacted] as:

[redacted] b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

~~(TS//STLW//SI//OC/NF)~~ Other examples of PSP successes cited in IC records and briefings include the [redacted] cases.

[redacted] PSP analysis and reporting helped to identify and locate [redacted] who was arrested in [redacted] Subsequent PSP analysis of [redacted] identified [redacted] This information generated several leads for the FBI. b1, b3, b6, b7C, b7E

~~(TS//STLW//SI//OC/NF)~~ [redacted] According to internal FBI briefing materials, PSP reporting was "instrumental in [redacted] becoming the subject of a Full Investigation [redacted]." However, the FBI's Counterterrorism Division told the DoJ OIG that "no [redacted] reporting factored into [redacted] investigation." b1, b3, b6, b7C, b7E

[redacted] PSP reporting assisted in locating his network's worldwide associates [redacted]

[redacted]

[redacted]

(U) ATTORNEY GENERAL GONZALES'S TESTIMONY ON THE PRESIDENT'S SURVEILLANCE PROGRAM

(U) As part of this review, the DoJ IG examined whether Attorney General Gonzales made false, inaccurate, or misleading statements to Congress related to the PSP. Aspects of the PSP were first disclosed publicly in a series of articles in *The New York Times* in December 2005. In response, the President publicly confirmed a portion of the PSP—which he called the terrorist surveillance program—describing it as the interception of the content of international communications of people reasonably believed to have links to al-Qaeda and related organizations. Subsequently, Gonzales was questioned about NSA surveillance activities in two hearings before the Senate Judiciary Committee in February 2006 and July 2007.

~~(S//NF)~~ Through media accounts and Comey's Senate Judiciary Committee testimony in May 2007, it was publicly revealed that DoJ and the White House had a major disagreement related to the PSP, which brought several senior DoJ and FBI officials to the brink of resignation in March 2004. In his testimony before the Senate Judiciary Committee, Gonzales stated that the dispute at issue between DoJ and the White House did not relate to the "Terrorist Surveillance Program" that the President had confirmed, but rather pertained to other intelligence activities. We believe this testimony created the misimpression that the dispute concerned activities entirely unrelated to the terrorist surveillance program, which was not accurate. In addition, we believe Gonzales's testimony that DoJ attorneys did not have "reservations" or "concerns" about the program the "President has confirmed" was incomplete and confusing [redacted] and that these concerns had been conveyed to the White House over a period of months before the issue was resolved.

(b) (5), (b)(1), (b)(3)

~~(S//NF)~~ The DoJ IG recognizes that Gonzales was in the difficult position of testifying about a highly classified program in an open forum. However, Gonzales, as a participant in the March 2004 dispute between DoJ and the White House and, more importantly, as the nation's chief law enforcement officer, had a duty to balance his obligation not to disclose classified information with the need not to be misleading in his testimony. Although we believe that Gonzales did not intend to mislead Congress, we believe his testimony was confusing, inaccurate, and had the effect of misleading those who were not knowledgeable about the program.

(U) CONCLUSIONS

(U) Pursuant to Title III of the FISA Amendments Act of 2008, the Inspectors General of the DoD, the DoJ, the CIA, the NSA, and the ODNI conducted reviews of the PSP. In this report and the accompanying individual reports of the participating IGs, we describe how, following the terrorist attacks of 11 September 2001, the President enhanced the NSA's SIGINT collection authorities in an effort to "detect and prevent acts of terrorism against the United States."

~~(TS//SI//NF)~~ Pursuant to this authority, the NSA, [redacted] collected significant new information, such as the content of communications into and out of the United States, where one party to the communication was reasonably believed to be a member of al-Qa'ida, or its affiliates, or a group the President determined was in armed conflict with the United States. In addition, the President authorized the collection of significant amounts of telephony and Internet metadata. The NSA analyzed this information for dissemination as leads to the IC, principally the CIA and the FBI. As described in the IG reports, the scope of this collection authority changed over the course of the PSP.

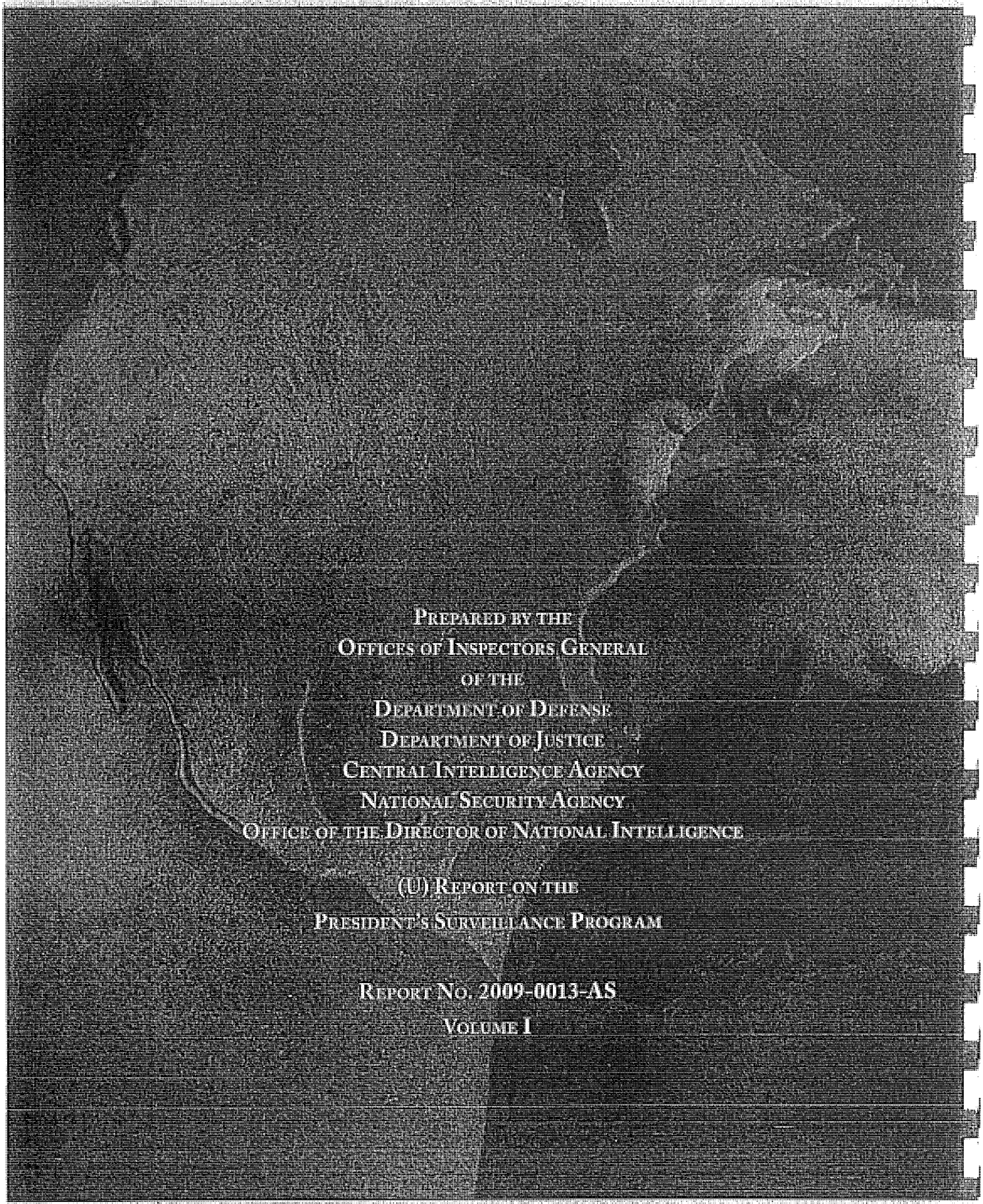
(U//~~FOUO~~) The IG reports describe the role of each of the participating agencies in the PSP, including the NSA's management and oversight of the collection, analysis, and reporting process; the CIA's and FBI's use of the PSP-derived intelligence in their counterterrorism efforts; the ODNI's support of the program by providing periodic threat assessments; and the DoJ's role in analyzing and certifying the legality of the PSP and managing use of PSP information in the judicial process.

(U) The IG reports also describe the conflicting views surrounding the legality of aspects of the PSP during 2003 and 2004, the confrontation between officials from DoJ and the White House about the legal basis for parts of the program and the resolution of that conflict. The ensuing transition of the PSP, in stages, from presidential authority to statutory authority under FISA, is also described in the IG reports.

(U) The IGs also examined the impact of PSP information on counterterrorism efforts. Many senior IC officials believe that the PSP filled a gap in intelligence collection thought to exist under FISA by increasing access to international communications that transited domestic U.S. communication wires, particularly international communications that originated or terminated within the United States. Others within the IC Community, including FBI agents, CIA analysts and managers, and other officials had difficulty evaluating the precise contribution of the PSP to counterterrorism efforts because it was most often viewed as one source among many available analytic and intelligence-gathering tools in these efforts. The IG reports describe several examples of how PSP-derived information factored into specific investigations and operations.

(U) The collection activities pursued under the PSP, and under FISA following the activities' transition to operation under that authority, as described in this report, resulted in unprecedented collection of communications content and metadata. We believe the retention and use by IC organizations of information collected under the PSP and FISA, particularly information on U.S. persons, should be carefully monitored.

This page intentionally left blank.



PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

(U) REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

REPORT NO. 2009-0013-AS
VOLUME I

(U) ANNEX TO THE REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

VOLUME II

10 JULY 2009

PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Special Warning

The report contains compartmented, classified material and no secondary distribution may be made without prior consent of the participating Inspectors General. Improper disclosure of this report may result in criminal, civil, or administrative penalties.

REPORT NO. 2009-0013-A

(U) Table of Contents

(U) The Deparment of Defense Inspector General's Review of the President's Surveillance Program 1

~~(S//NF)~~ The Central Intelligence Agency Inspector General's Review of CIA Participation in the President's Surveillance Program 11

(U) The National Security Agency, Central Security Service Inspector General's Review of the President's Surveillance Program 45

~~(S//NF)~~ The Office of the Director of National Intelligence Inspector General's Review of the Participation of the ODNI in the President's Surveillance Program 213

This page intentionally left blank.

~~TOP SECRET//STLW//SI//ORCON//NOFORN~~
~~SPECIAL ACCESS REQUIRED~~

Report No. 09-INTEL-03
27 March 2009
(Project

Inspector General
United States
Department of Defense

DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

Review of the President's Surveillance Program (U)

~~Derived From: Multiple Sources~~
~~Declassify On: 20340511*~~

Copy ____ of ____

This page intentionally left blank.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

June 26, 2009

MEMORANDUM FOR SECRETARY OF DEFENSE

SUBJECT: (U) Report on Review of the President's Surveillance Program Report No.: 09-INTEL-08 (U)

(U) We are providing this report for your information. This report fulfills the DoD Inspector General's requirement pursuant to Section 301 of Public Law 110-261, the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 (the Act). This report, along with reports prepared by the Inspectors General of the Department of Justice (DoJ), the Office of the Director of National Intelligence (DNI), Central Intelligence Agency (CIA), the National Security Agency (NSA), will be summarized in a comprehensive report as required by the Act.

~~(TS//STLW//SI//OC//NF)~~ **Results.** The OSD role in the establishment and implementation of the PSP was limited, with the burden of program execution residing with the NSA. We determined that there were six OSD officials with access to the PSP. These individuals had limited involvement, and did not make any additional tasking decisions beyond those directed for NSA implementation. We are aware of no other OSD involvement in the PSP.

(U) Background. The Act requires the IGs of the DoJ, DNI, NSA, the DoD, and any other element of the intelligence community that participated in the President's Surveillance Program (PSP)[1], to complete a comprehensive review of, with respect to the oversight authority and responsibility of each such IG:

- All facts necessary to describe establishment, implementation, product and use of the product in the program
- Access to legal reviews and access to information about the Program
- Communications and participation of individuals/entities related to the Program

[1] (U) The President's Surveillance Program is defined in the Act as the intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005 (commonly known as the Terrorist Surveillance Program).

~~Derived from: Multiple Sources~~
~~Declassify on: 20340511*~~

- Interaction with the Foreign Intelligence Surveillance Court and
- Any other matters identified by the IGs

~~(TS//STLW//SI//OC//NF)~~ **Scope and Methodology.** We conducted this review to examine the involvement of the Office of the Secretary of Defense (OSD), Department of Defense (DoD), in the establishment and implementation of the President's Surveillance Program (PSP). We interviewed current and former officials within OSD that had access to the PSP. We withdrew our request to interview Secretary of Defense Gates because he was provided access to the PSP after the program ended. The former Deputy Secretary of Defense Dr. Wolfowitz declined our request for an interview. We reviewed all relevant documentation within OSD and NSA related to OSD's involvement in the PSP. We also reviewed documentation at DoJ related to the PSP.

(U) The IGs of the DoJ, DoD, DNI, NSA, and CIA issued an interim report on September 10, 2008. In the interim report, the DoD IG stated that he would examine the involvement of the Office of the Secretary of Defense (OSD) in the establishment and implementation of the PSP. The NSA, as an agency within DoD performed the requirements of the PSP. As such, the NSA IG is conducting a review of NSA involvement with the PSP separate from this memorandum report.

~~(TS//STLW//SI//OC//NF)~~ **Implementation and Establishment of the PSP.** The OSD access to the PSP was limited to six individuals.[2] Those individuals are Secretary of Defense Robert Gates; former Secretary of Defense Donald Rumsfeld; former Deputy Secretary of Defense Paul Wolfowitz; Under Secretary of Defense for Intelligence (USD(I)) James Clapper[3]; former USD(I) Stephen Cambone; and Principal Deputy General Counsel Daniel Dell 'Orto.

~~(TS//STLW//SI//OC//NF)~~ The PSP was an extremely sensitive counterterrorism program focused on detecting and preventing terrorist attacks within the United States. The PSP was authorized by the President every 30 to 45 days and was initially directed against international terrorism; after March 2004, the PSP focused specifically against al-Qaeda and its affiliates. The Director of Central Intelligence (DCI), and later the DNI, would prepare a Threat Assessment

[redacted]

[3] ~~(TS//STLW//SI//OC//NF)~~ Secretary Gates and Under Secretary Clapper were provided access to the PSP after the PSP was transferred to Foreign Intelligence Surveillance Court supervision.

Memorandum, which validated the current threat to the United States. The Secretary of Defense would review and sign the Threat Assessment Memorandum. On three occasions, Dr. Wolfowitz, the former Deputy Secretary of Defense, signed the Threat Assessment Memoranda in the Secretary's absence. On two occasions, Dr. Cambone, the former USD(I), signed the Threat Assessment Memoranda when Secretary Rumsfeld and Dr. Wolfowitz were unavailable.

~~(TS//STLW//SI//OC//NF)~~ Once the Threat Assessment Memorandum was signed, the President would then sign a Presidential Authorization with the Threat Memorandum attached. The President would task the Secretary of Defense to employ DoD resources to execute the requirements set forth in the Presidential Authorization. The Attorney General, or his designee, would certify the Presidential Authorization for form and legality. The Secretary of Defense would then direct the actions authorized by the Presidential Authorization to the NSA for implementation. On one occasion, Dr. Wolfowitz, the former Deputy Secretary of Defense, directed the Director of NSA to implement the Presidential Authorization, in the Secretary's absence. On a separate occasion, Dr. Cambone, the former USD(I), directed the Director of NSA to implement the Presidential Authorization.

~~(TS//SI//NF)~~ **Interaction with the Foreign Intelligence Surveillance Court.** Dr. Wolfowitz also executed two declarations to the U.S. Foreign Intelligence Surveillance Court. The first, executed on [redacted] was in support of the Government's Application seeking renewal, in part, of the authority to install and use pen register and trap and trace devices, in order to obtain information [redacted] pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. sections 1801-1811, 1841-1846, as amended. The initial authority under FISA to install and use pen register and trap and trace devices for that purpose was granted by the Foreign Intelligence Surveillance Court on July 14, 2004. [redacted]

~~(TS//SI//NF)~~ Dr. Wolfowitz's second declaration was executed on [redacted] That declaration was made in response to the Foreign Intelligence Surveillance Court's [redacted] Order requiring the Government to submit a declaration from the Deputy Secretary of Defense discussing NSA' violations of the Court's July 14 Order authorizing NSA to install and use pen register and trap and trace devices in order to obtain information about [redacted]. In that declaration, Dr. Wolfowitz stated the circumstances surrounding unauthorized collection that occurred, the disposition of information collected without authorization, steps NSA took to remedy the violation, and measures NSA implemented to prevent recurrence of such violations.

(TS//STLW//SI//ORCON/NOFORN)

(U) Should you have questions on this memo, please feel free to contact [illegible], Patricia A. Dunmire at (703) 613-8879.

[illegible]

APPENDIX (U)

REPORT DISTRIBUTION LIST (U)

(U)

OFFICE OF THE SECRETARY OF DEFENSE

Secretary of Defense
Under Secretary of Defense for Intelligence
Deputy General Counsel, Intelligence

OTHER DEFENSE ORGANIZATION

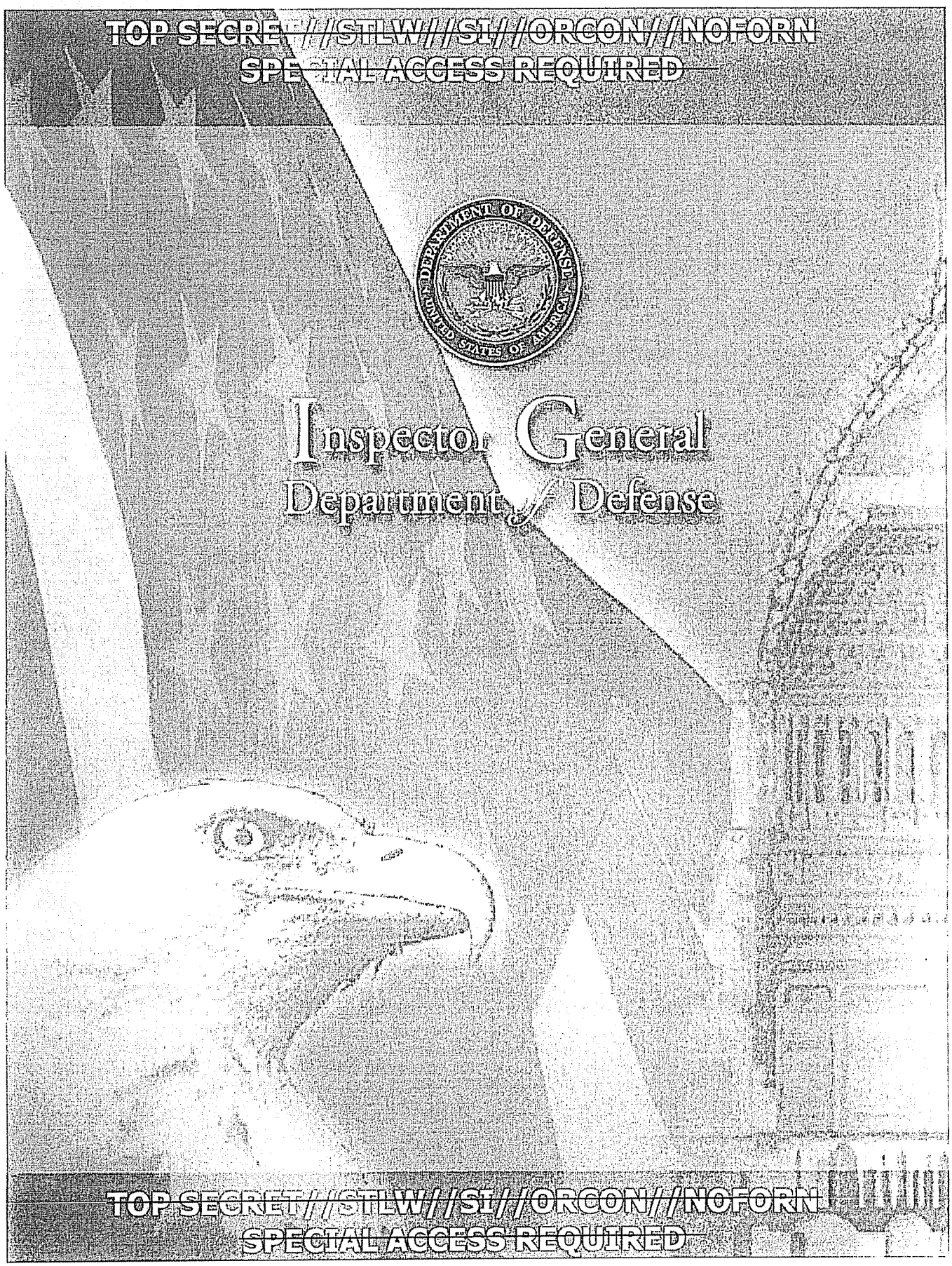
Inspector General, National Security Agency

NON-DEFENSE FEDERAL ORGANIZATIONS

Inspector General, Director of National Intelligence
Inspector General, Department of Justice
Inspector General, Central Intelligence Agency

CONGRESSIONAL COMMITTEES

Senate Judiciary Committee
Senate Select Committee on Intelligence
House Judiciary Committee
House Permanent Select Committee on Intelligence


TOP SECRET//STLW//SI//ORCON//NOFORN
SPECIAL ACCESS REQUIRED
Inspector General
Department of Defense
TOP SECRET//STLW//SI//ORCON//NOFORN
SPECIAL ACCESS REQUIRED

This page intentionally left blank.

This page intentionally left blank.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

CENTRAL INTELLIGENCE AGENCY

Office of Inspector General

(U) FINAL REPORT

~~(S//NF)~~ CIA Participation in the President's Surveillance Program

Report No. 2008-0016-AS

[redacted]

30 June 2009

Issue Date

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

This page intentionally left blank.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

(U) Table of Contents

(U) EXECUTIVE SUMMARY 1

(U) BACKGROUND 3

(U) Origin and Scope of the Review 4

(U) The President's Surveillance Program 5

(U) REVIEW RESULTS 6

~~(S//NF)~~ CIA Participation in the President's Surveillance Program 6

~~(TS//STLW//SI//OC/NF)~~ CIA Prepared the Threat Assessment Memorandums Supporting Authorization of the President's Surveillance Program 7

(U//~~FOUO~~) CIA Tasked and Received Reporting From the President's Surveillance Program 9

(U//~~FOUO~~) Procedures and Standards for Requesting Information 9

(U//~~FOUO~~) Reporting Provided in Response to Requests for Information 10

(U//~~FOUO~~) Primary CIA Users of the President's Surveillance Program 11

(U//~~FOUO~~) CIA Requests for Information Were Adequately Justified 13

(U//~~FOUO~~) Senior CIA Officials Believe That the President's Surveillance Program Filled an Intelligence Gap 13

(U//~~FOUO~~) The CIA Did Not Assess the Effectiveness of the President's Surveillance Program 15

(U) Counterterrorism Successes Supported by the President's Surveillance Program 16

~~(S//NF)~~ Several Factors Hindered CIA Utilization of the President's Surveillance Program 17

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

(U) CIA Had Limited Access to Legal Reviews of the President's Surveillance Program 19

~~(S//NF)~~ CIA Officials Sought to Delay Exposure of the President's Surveillance Program by the *New York Times* 20

(U) Methodology ..... Exhibit A

(U) Threat Assessment Memorandum Concluding Paragraph ..... Exhibit B

(U) Example of Link Diagram From August 2002 ..... Exhibit C

(U) Review Team ..... Exhibit D

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~(S//NF)~~ CIA Participation in the President's Surveillance Program

(U) EXECUTIVE SUMMARY

~~(S//NF)~~ Title III of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 requires the Inspectors General (IGs) of the elements of the Intelligence Community (IC) that participated in the President's Surveillance Program (PSP) to conduct a comprehensive review of the program. The results of our review of CIA participation in the PSP are presented in this report, and will be included in the comprehensive report required to be provided to the appropriate committees of Congress by 10 July 2009.

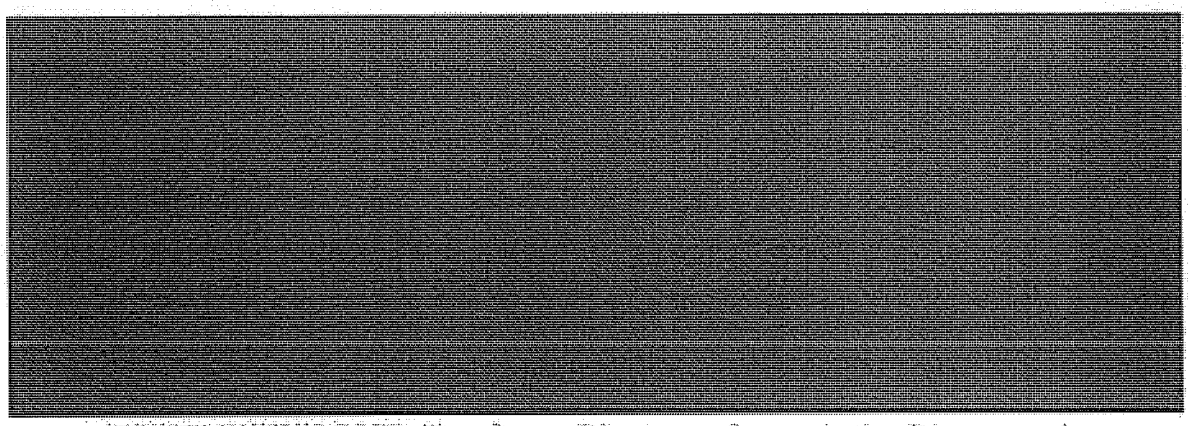
~~(TS//STLW//SI//OC/NF)~~ The CIA prepared the threat assessment memorandums that were used to support Presidential authorization and periodic reauthorizations of the PSP. The threat assessment memorandums were prepared by personnel from the CIA [redacted] Each of the memorandums focused on the current threat situation and did not provide an assessment of the PSP's utility in addressing previously reported threats. The threat assessment memorandums were signed by the Director of Central Intelligence (DCI) and forwarded to the Secretary of Defense to be co-signed. Responsibility for drafting the threat assessment memorandums was transferred to the newly-established Terrorist Threat Integration Center in May 2003 and retained by TTIC's successor organization, NCTC (the National Counterterrorism Center). The DCI continued to sign the threat assessment memorandums through 15 April 2005. Subsequent memorandums were signed by the Director of National Intelligence.

~~(TS//STLW//SI//OC/NF)~~ CIA analysts and targeters, as PSP consumers, tasked the program and utilized the product from the program in their analyses. [redacted]

1

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~



~~(TS//STLW//SI//OC/NF)~~ Two former Directors, a former Acting Director, and other senior CIA officials we interviewed told us that the PSP addressed a gap in intelligence collection. [redacted] However, collection of such communications required authorization under FISA, and there was widespread belief among senior IC and CIA officials that the process for obtaining FISA authorization was too cumbersome and time consuming to address the current threat. Current and former CIA officials emphasized the increased timeliness, flexibility, and access provided by the PSP as compared to the process for obtaining a warrant under FISA.

~~(TS//STLW//SI//OC/NF)~~ The CIA did not implement procedures to assess the usefulness of the product of the PSP and did not routinely document whether particular PSP reporting had contributed to successful counterterrorism operations. CIA officials told us that PSP reporting was used in conjunction with reporting from other intelligence sources and was rarely the sole basis for a counterterrorism success. [redacted] CIA officers, even those read into the program, would have been unaware of the full extent of PSP reporting. Consequently, there is no means to comprehensively track how PSP information was used. CIA officials were able to provide only limited information on how program reporting contributed to successful operations, and therefore, we were unable to independently draw any conclusion on the overall usefulness of the program to CIA.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~(S//NF)~~ Several factors hindered the CIA in making full use of the capabilities of the PSP. Many CIA officials told us that too few CIA personnel at the working level were read into the PSP. [redacted] officials told us that CIA analysts and targeting officers who were read in had too many competing priorities and too many other available information sources and analytic tools—many of which were more easily accessed and timely—to fully utilize the PSP. CIA officers also told us that the PSP would have been more fully utilized if analysts and targeting officers had obtained a better understanding of the program's capabilities. Many CIA officers noted that there was insufficient training and legal guidance concerning the program's capabilities and the use of PSP-derived information. The factors that hindered the CIA in making full use of the PSP might have been mitigated if the CIA had designated an individual at an appropriate level of managerial authority, who possessed knowledge of both the PSP and CIA counterterrorism activities, to be responsible and accountable for overseeing CIA participation in the program.

~~(TS//STLW//SI//OC/NF)~~ There is no indication that personnel from the CIA Office of General Counsel or other CIA components were involved in preparing the legal memorandums supporting the PSP that were produced by the Department of Justice, Office of Legal Counsel (OLC). CIA OGC personnel had very limited access to these memorandums.

~~(S//NF)~~ Senior CIA officials participated in meetings with a *New York Times* editor and reporter and senior Administration officials concerning an article the newspaper was preparing concerning the PSP.

[redacted]
Assistant Inspector General for Audit

This page intentionally left blank.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

(U) BACKGROUND

(U) Origin and Scope of the Review

(U) Title III of the Foreign Intelligence Surveillance Act Amendments Act of 2008, which was signed into law on 10 July 2008, requires the IGs of the elements of the Intelligence Community that participated in the PSP to conduct a comprehensive review of the program.[1] The review required to be conducted under the Act is to examine:

> (A) all of the facts necessary to describe the establishment, implementation, product, and use of the product of the Program;
>
> (B) access to legal reviews of the program and access to information about the Program;
>
> (C) communications with, and participation of, individuals and entities in the private sector related to the Program;
>
> (D) interaction with the Foreign Intelligence Surveillance Court and transition to court orders related to the Program; and
>
> (E) any other matters identified by any such Inspector General that would enable that Inspector General to complete a review of the Program, with respect to such Department or element.

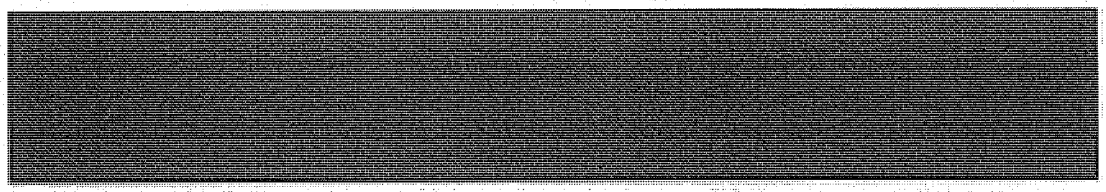
~~(TS//STLW//SI//OC/NF)~~ The interim report required under the Act was submitted to the committees of Congress prescribed in the Act on 10 September 2008. That report described the scope of the work to be conducted by each of the participating IGs, which include the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and the CIA. Our review of CIA participation in the PSP examined CIA's :

- Role in preparing the threat assessments and legal certifications supporting periodic reauthorization of the PSP.
- Role in identifying targets for the PSP.

---

[1] ~~(S//NF)~~ The President's Surveillance Program is defined in the Act as the intelligence activity involving communications that was authorized by the President during the period beginning on 11 September 2001, and ending on 17 January 2007, including the program referred to by the President in a radio address on 17 December 2005 (commonly known as the Terrorist Surveillance Program). The classified name for the President's Surveillance Program is "STELLARWIND."

~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~



The results of our review of CIA participation in the PSP are presented in this report, and will be included in the comprehensive final report required to be provided to the appropriate committees of Congress by 10 July 2009.

(U) The President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ According to former Director of the NSA and former Director of the CIA (DCIA) Michael V. Hayden, initial discussions concerning the activities that would become the PSP occurred less than two weeks after the 11 September 2001 terrorist attacks in a meeting between DCI George J. Tenet and Vice President Richard B. Cheney. Although Hayden did not attend the meeting, he was told by Tenet that Cheney asked if the Intelligence Community was doing everything possible to prevent another terrorist attack. In response, Tenet described

Cheney then asked if there was more that NSA could do. This led to discussions between Cheney, Hayden, Cheney's legal counsel David S. Addington, and senior NSA officials. It was determined that the NSA had the capability to collect additional wire communications that could enhance the IC's counterterrorism efforts, but that new authority was needed to employ the capability. The determination led to the authorization of the PSP by President George W. Bush on 4 October 2001.

~~(TS//STLW//SI//OC/NF)~~ The PSP was intended to help prevent additional terrorist attacks against the US Homeland. Although the authorized collection activities changed over the life of the program, in general, the program authorized the NSA to acquire content and/or metadata concerning telephone and e-mail communications for which there were reasonable grounds to believe that at least one of the participants in the communication was located outside the US and that a party to

~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~

the communication was affiliated with a group engaged in international terrorism. The collection activities conducted under the PSP were brought under Foreign Intelligence Surveillance Court oversight in stages between July 2004 and January 2007.[2]

~~(TS//STLW//SI//OC/NF)~~ Under the PSP, the NSA collected three sets of data. The first set included the content of individually targeted telephone and e-mail communications. The second set consisted of telephone dialing information—the date, time, and duration of calls; the telephone number of the caller; and the number receiving the call—collected in bulk [redacted] The third data set consisted of e-mail transactional data—[redacted] collected in bulk [redacted]

(U) REVIEW RESULTS

~~(S//NF)~~ CIA Participation in the President's Surveillance Program

[redacted]

[2] (U) The Foreign Intelligence Surveillance Act of 1978 established the Foreign Intelligence Surveillance Court to oversee requests for surveillance warrants by federal agencies against suspected foreign intelligence agents inside the US.

~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

[redacted]

~~(TS//STLW//SI//OC/NF)~~ [redacted] CIA personnel prepared the threat assessment memorandums that were used to support the initial Presidential authorization and subsequent reauthorizations of the PSP. [redacted]

~~(TS//STLW//SI//OC/NF)~~ CIA Prepared the Threat Assessment Memorandums Supporting Authorization of the President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ The CIA initially prepared the threat assessment memorandums that were used to support Presidential authorization and periodic reauthorizations of the PSP. The memorandums documented the current threat to the US homeland and to US interests abroad from al-Qa'ida and affiliated terrorist organizations. The first threat assessment memorandum—*The Continuing Near-Term Threat from Usama Bin Ladin*—was signed by DCI Tenet on 4 October 2001.[3] Subsequent threat assessment memorandums were prepared every 30 to 60 days to correspond with the President's reauthorizations of the PSP.

~~(TS//STLW//SI//OC/NF)~~ The DCI Chief of Staff, John H. Moseman, was the CIA focal point for preparing the threat assessment memorandums. According to Moseman, he directed the [redacted] to prepare objective appraisals of the current terrorist threat, focusing primarily on threats to the homeland, and to document those appraisals in a memorandum. Initially, the [redacted] analysts who prepared the threat assessments were not read into the PSP and did not know how the threat assessments would be used. [redacted] analysts drew upon all sources of intelligence in preparing their threat assessments. Each of the memorandums focused on the current threat situation and did not provide an assessment of the PSP's utility in addressing previously reported threats.

---

[3] ~~(S//NF)~~ The title of the threat assessment memorandums was changed to *The Global War Against Terrorism* in June 2002.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~(TS//STLW//SI//OC/NF)~~ After [redacted] completed its portion of the memorandums, the DCI's Chief of Staff added a paragraph at the end of the memorandums stating that the individuals and organizations involved in global terrorism (and discussed in the memorandums) possessed the capability and intention to undertake further terrorist attacks within the US. Moseman recalled that the paragraph was provided to him initially by either White House Counsel Alberto R. Gonzales or Addington. The paragraph recommended that the President authorize the Secretary of Defense to employ within the US the capabilities of the Department of Defense, including but not limited to NSA's signals intelligence capabilities, to collect foreign intelligence by electronic surveillance. The paragraph also described the types of communication and data that would be collected and the circumstances under which they could be collected.[4] The draft threat assessment memorandums were then reviewed by Office of General Counsel attorneys assigned to [redacted] and Acting General Counsel (Senior Deputy General Counsel) John A. Rizzo. Rizzo told us that the draft memorandums were generally sufficient, but that there were occasions when, based on his experience with previous memorandums, he thought that draft memorandums contained insufficient threat information or did not present a compelling case for reauthorization of the PSP. In such instances, Rizzo would request tha[redacted] provide additional available threat information or make revisions to the draft memorandums.

~~(TS//STLW//SI//OC/NF)~~ The threat assessment memorandums were then signed by DCI Tenet and forwarded to the Secretary of Defense to be co-signed. Tenet signed most of the threat memorandums prepared during his tenure as DCI. On the few occasions when he was unavailable, the Deputy Director of Central Intelligence (DDCI), John E. McLaughlin, signed the memorandums on behalf of Tenet. McLaughlin also signed the memorandums in the capacity of Acting DCI in August and September 2004. In November 2004, Porter J. Goss became DCI and assumed responsibility for signing the memorandums. There were no occasions when the DCI or Acting DCI withheld his signature from the threat assessment memorandum. After they were signed by the Secretary of Defense, the memorandums were reviewed by the Attorney General and delivered to the White House to be attached to the PSP reauthorization memorandums signed by the President.

~~(TS//STLW//SI//OC/NF)~~ Responsibility for drafting the threat assessment memorandums was transferred from [redacted] to the newly established Terrorist Threat Integration Center in May 2003. This responsibility was retained by TTIC's successor organization, NCTC. The DCI continued to sign the threat assessment memorandums

---

[4] (U) Exhibit B presents the conclusion and recommendation paragraph included in the threat assessment memorandum dated 10 January 2005. Similar language was included in each of the memorandums.

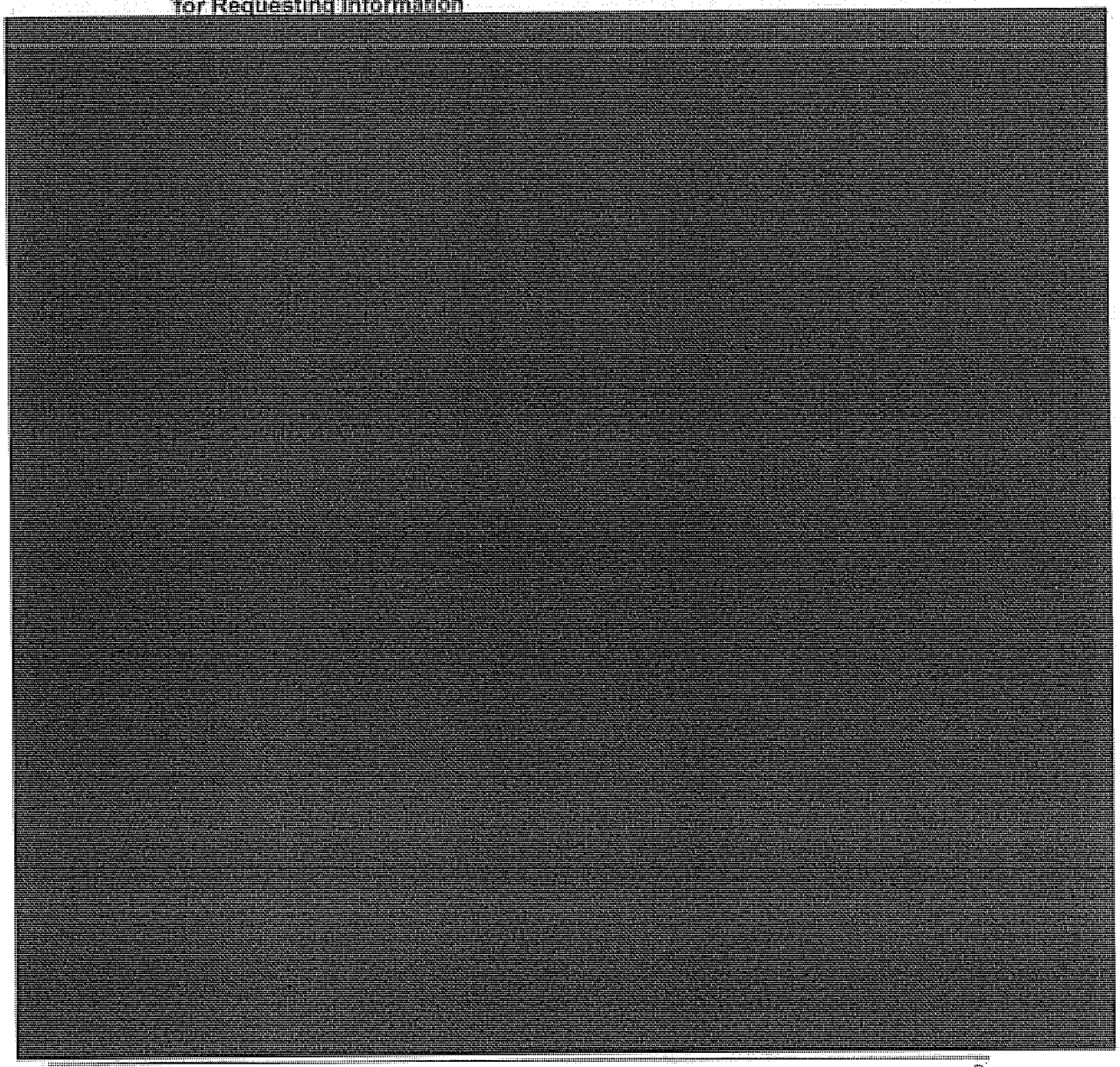
~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

through 15 April 2005. Subsequent memorandums were signed by the Director of National Intelligence.[5]

(U//~~FOUO~~) CIA Tasked and Received Reporting From the President's Surveillance Program

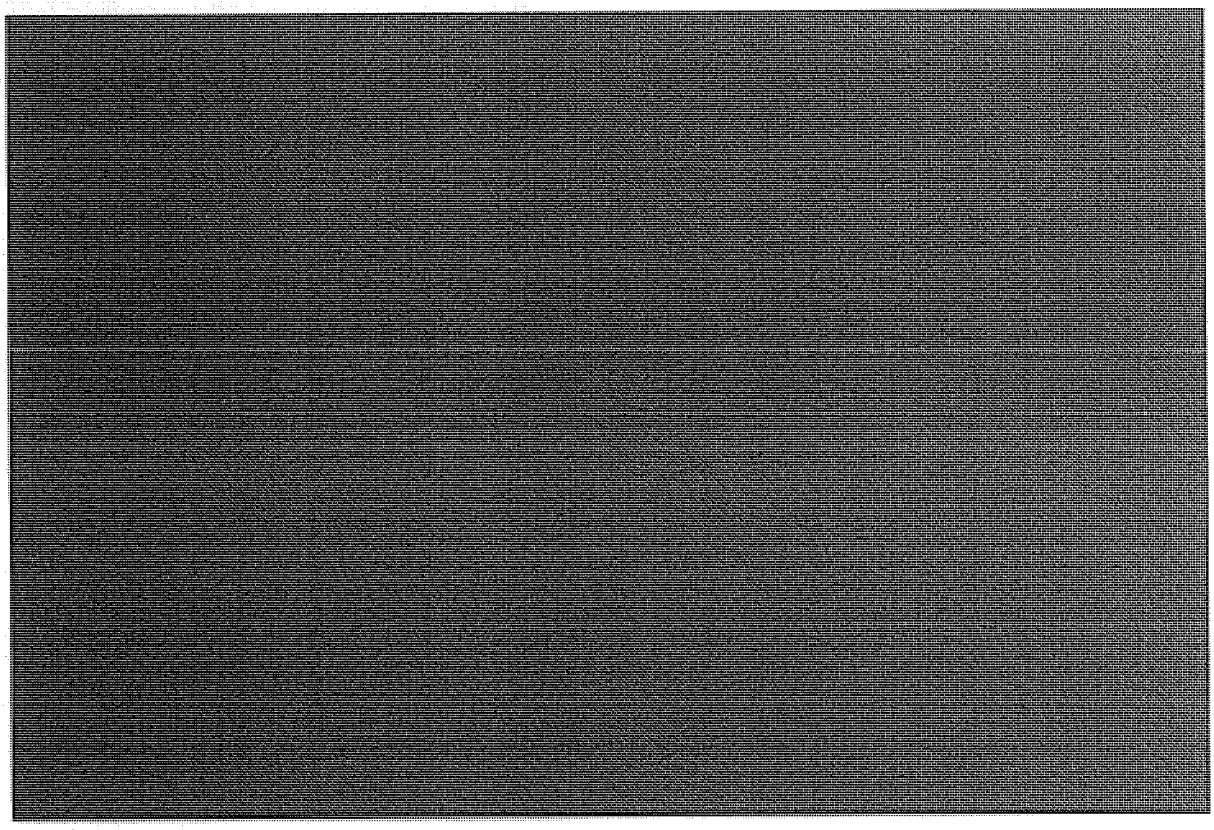
(U//~~FOUO~~) Procedures and Standards for Requesting Information



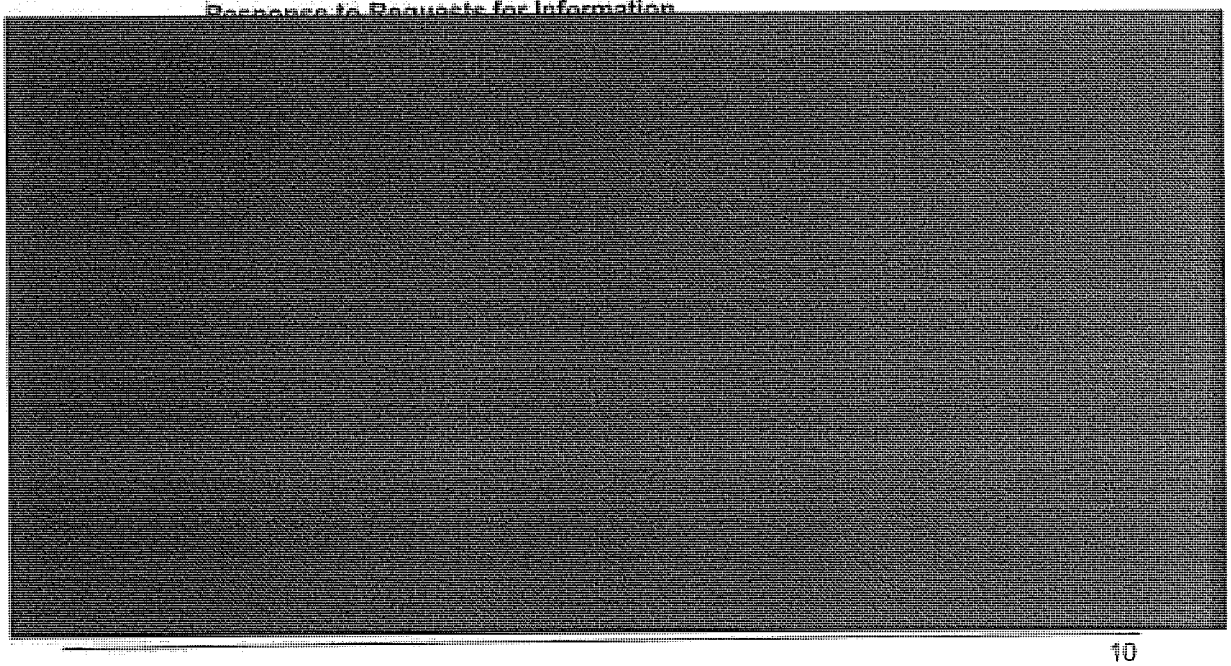
9

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//COMINT//ORCON/NOFORN~~



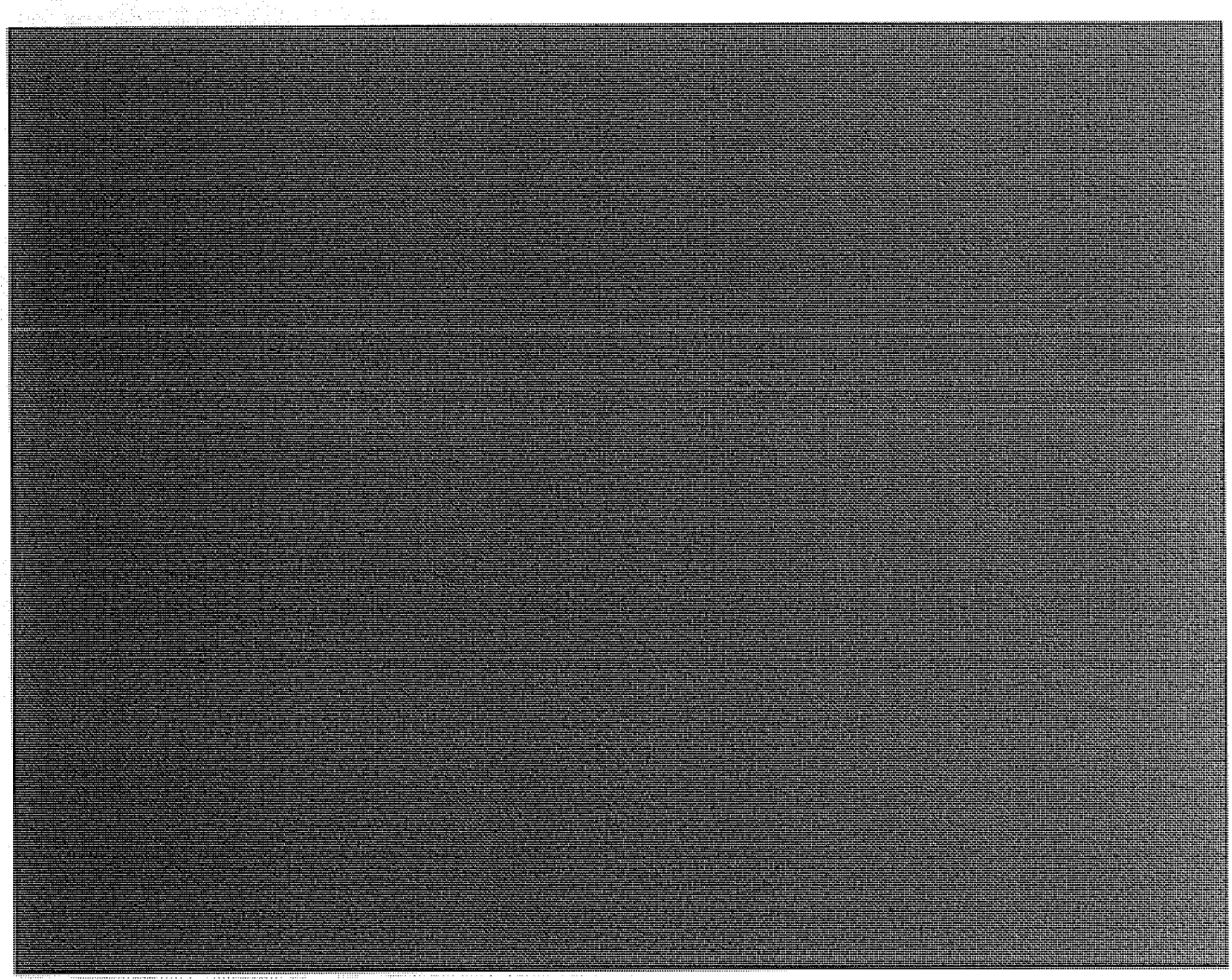
(U//FOUO) Reporting Provided in
Response to Requests for Information



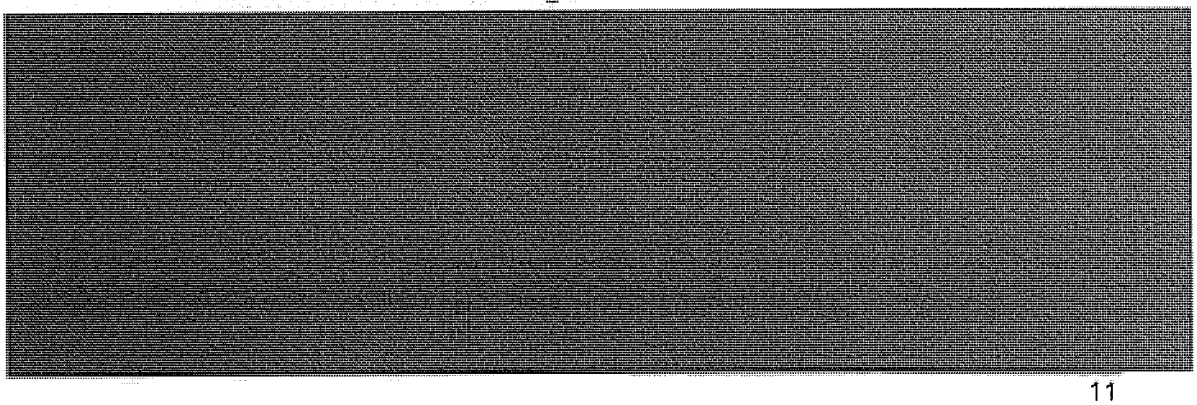
10

~~TOP SECRET//STLW//HCS//COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~



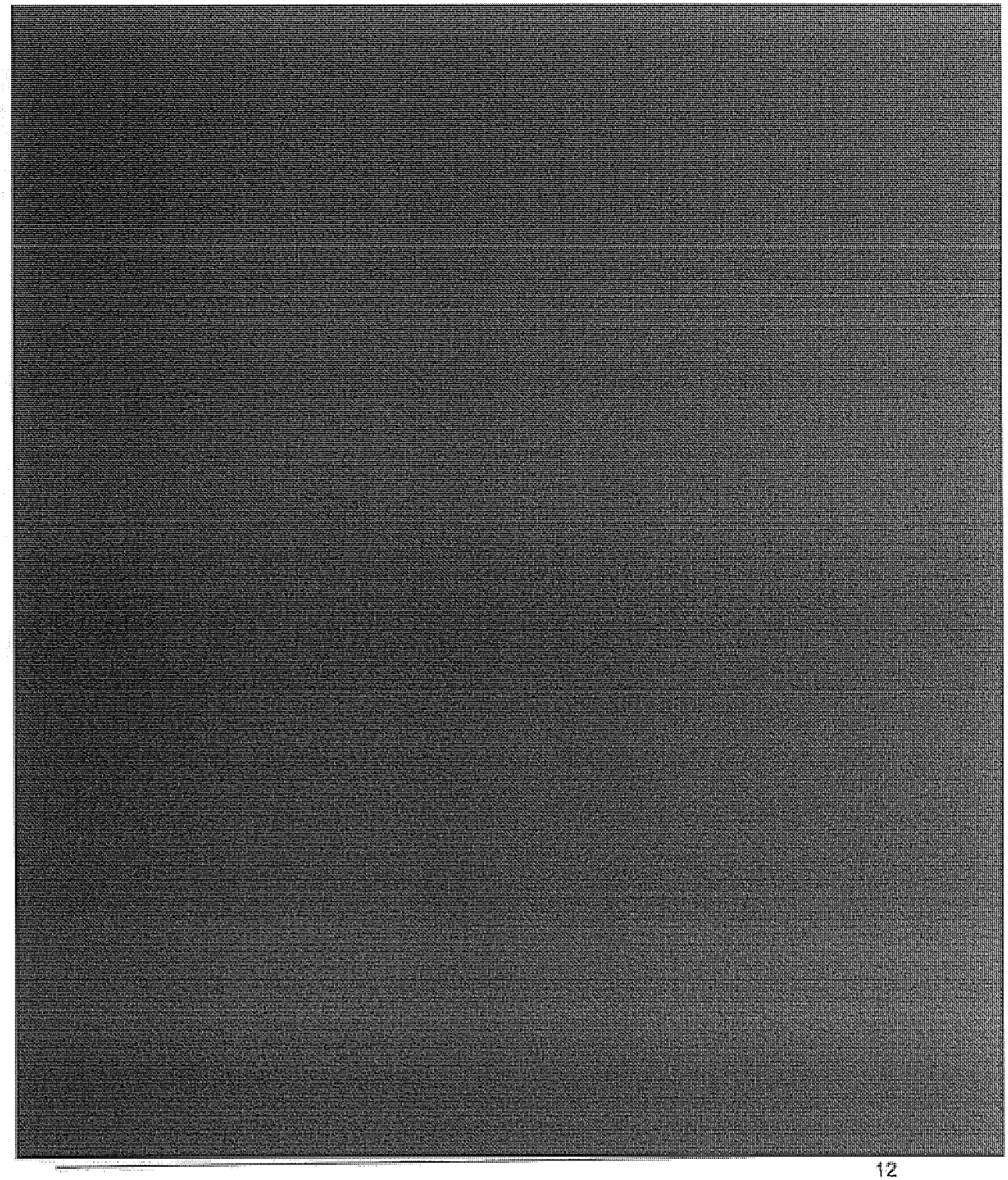
(U//~~FOUO~~) Primary CIA Users of the President's Surveillance Program



11

~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~

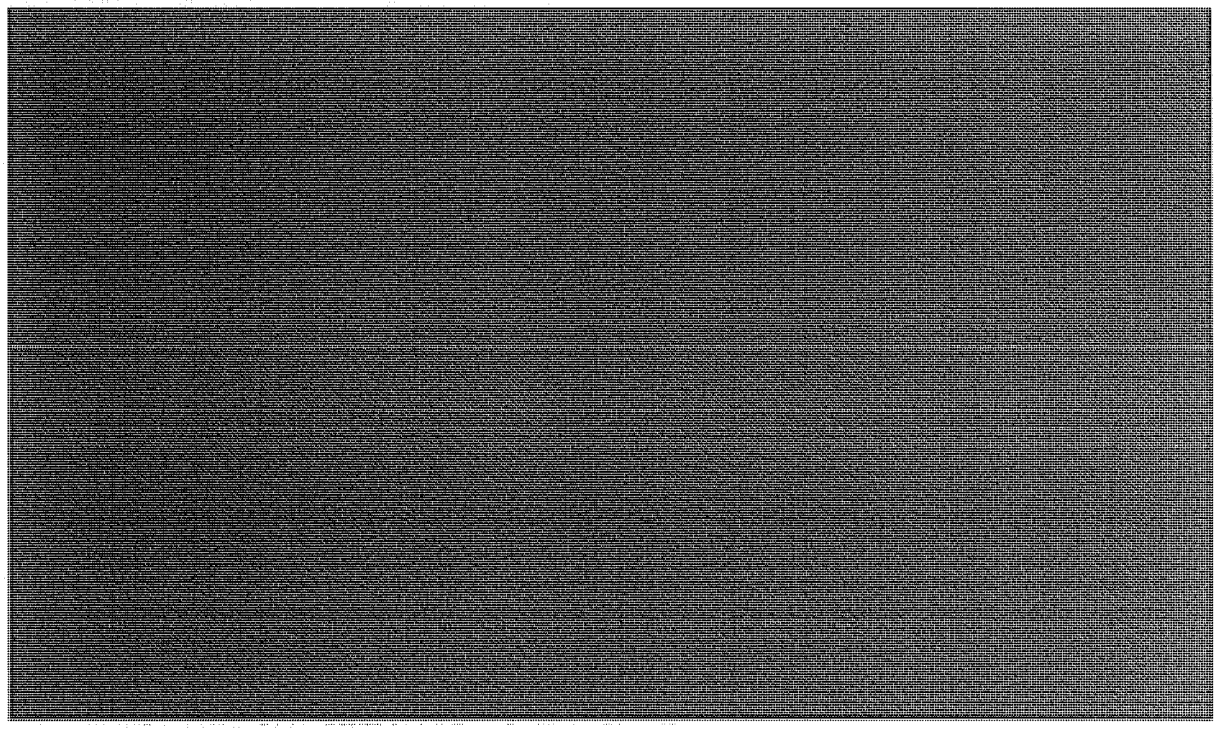
~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~



12

~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~



(U//~~FOUO~~) Senior CIA Officials Believe That the President's Surveillance Program Filled an Intelligence Gap

~~(TS//STLW//SI//OC/NF)~~ Former Directors Hayden and Goss, former Acting Director McLaughlin, and other senior CIA officials we interviewed told us that the PSP addressed a gap in intelligence collection. Following the terrorist attacks on 11 September 2001, there was concern that additional acts of terrorism would be perpetrated by terrorist cells already inside the US. [redacted] However, collection of such communications required authorization under FISA, and there was widespread belief among senior IC and CIA officials that the process for obtaining FISA authorization was too cumbersome and time consuming to address the current threat.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

[redacted]

~~(TS//STLW//SI/OC/NF)~~ Other senior CIA officials told us that the PSP provided CIA access to information that was previously unavailable. [redacted]

14

~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~

(U//~~FOUO~~) The CIA Did Not Assess the Effectiveness of the President's Surveillance Program

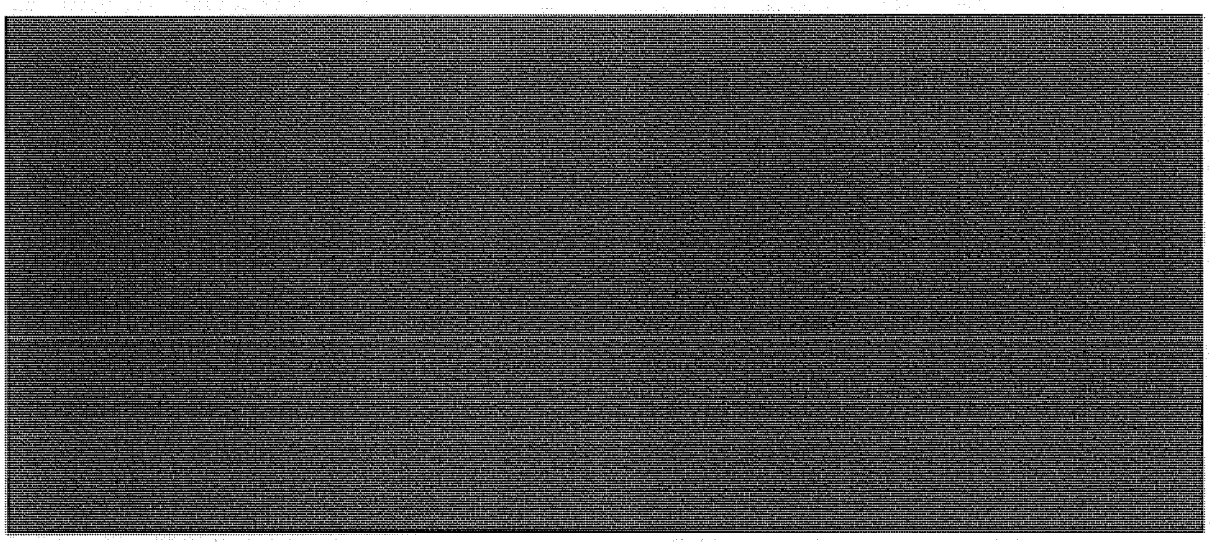
~~(TS//STLW//SI//OC/NF)~~ The CIA did not implement procedures to assess the usefulness of the product of the PSP and did not routinely document whether particular PSP reporting had contributed to successful counterterrorism operations. CIA officials, including DCIA Hayden, told us that PSP reporting was used in conjunction with reporting from other intelligence sources; consequently, it is difficult to attribute the success of particular counterterrorism operations exclusively to the PSP. In a May 2006 briefing to the Senate Select Committee on Intelligence (SSCI), the Deputy Director, [redacted] said that PSP reporting was rarely the sole basis for an intelligence success, but that it frequently played a supporting role. He went on to state that the program was an additional resource to enhance the CIA's understanding of terrorist networks and to help identify potential threats to the homeland. Other [redacted] officials we interviewed said that the PSP was one of many tools available to them, and that the tools were often used in combination.

[redacted]

15

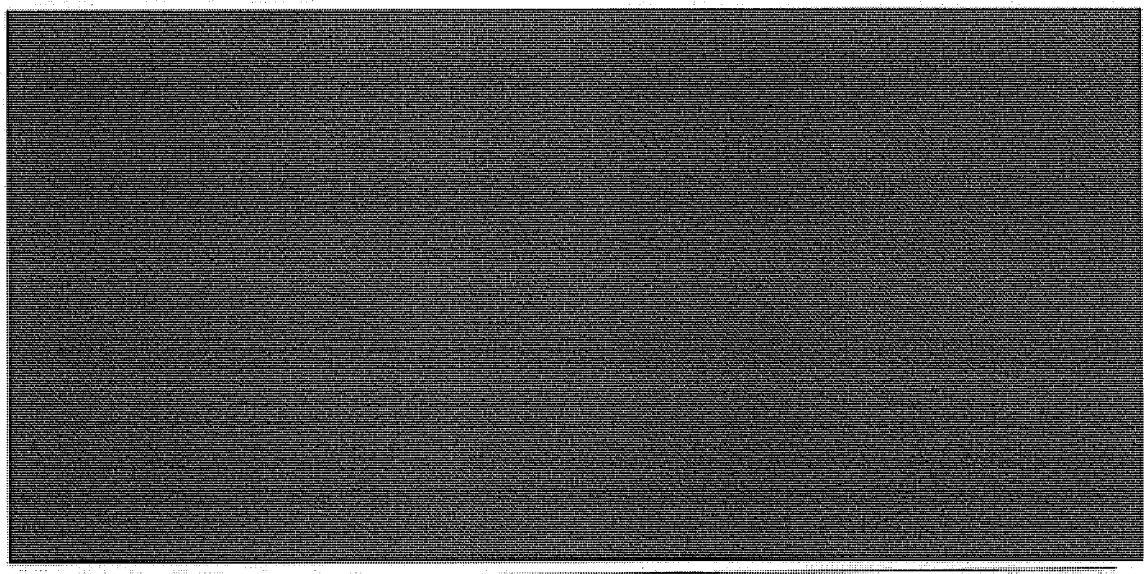
~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~

~~TOP SECRET//STLW//HCS//COMINT//ORCON/NOFORN~~



(U) Counterterrorism Successes Supported by the President's Surveillance Program

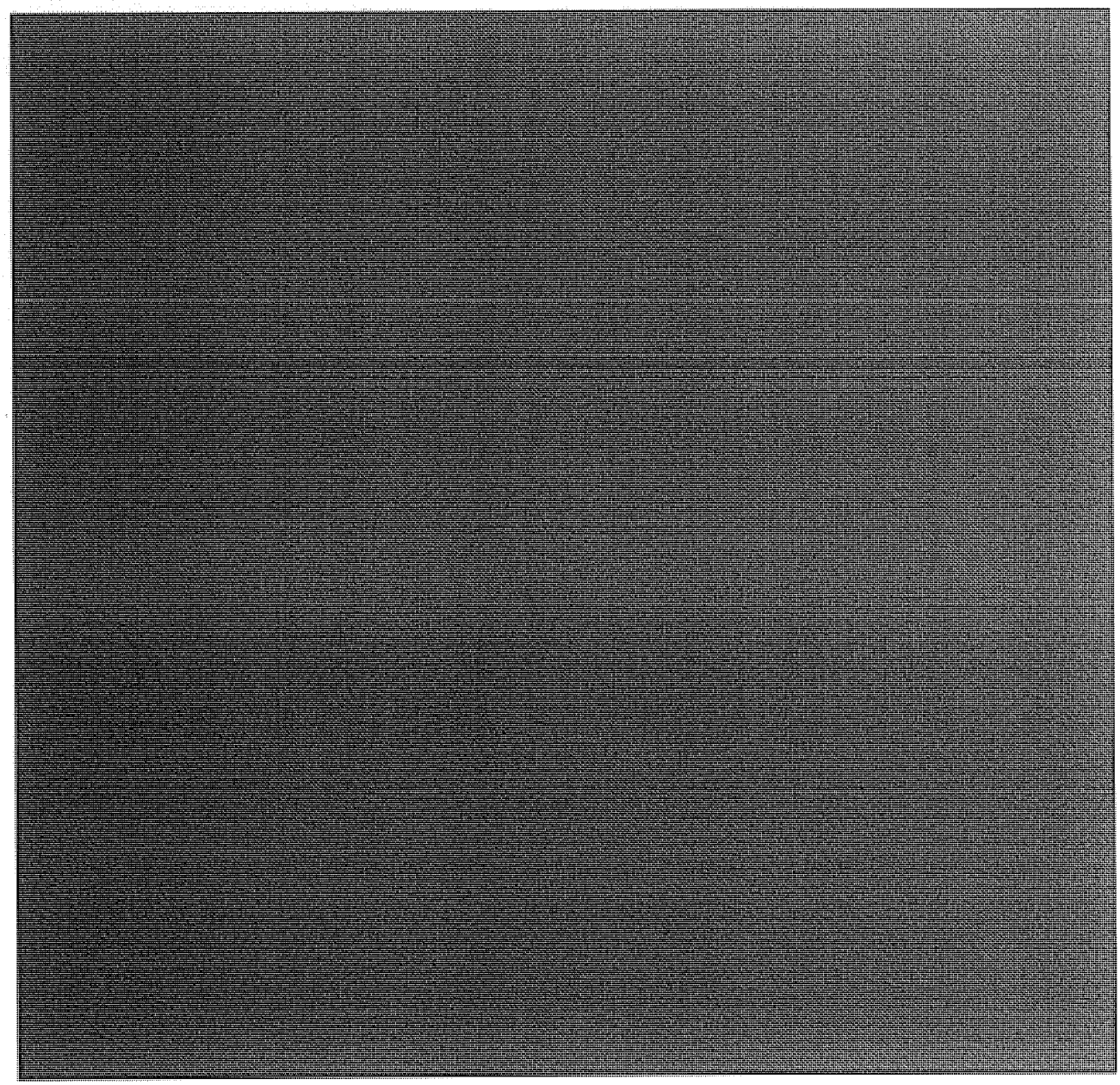
~~(S//NF)~~ Despite the fact that CIA officials we interviewed did not provide much specific information on PSP-derived counterterrorism successes, some key counterterrorism operations supported by the PSP were cited in briefings presented by CIA officials. In March 2004, the CIA provided a series of three briefings at the White House to senior Administration officials and Congressional leaders. These briefings included operational details concerning the PSP as well as examples of program successes. In May 2006, the Deputy Director, [redacted] briefed SSCI members and staff on the usefulness to [redacted] of the PSP.



~~TOP SECRET//STLW//HCS//COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~



~~(S//NF)~~ Several Factors Hindered CIA Utilization of the President's Surveillance Program

~~(S//NF)~~ Several factors hindered the CIA in making full use of the capabilities of the PSP. Many CIA officials told us that too few CIA personnel at the working level were read into the PSP. At the program's inception, a disproportionate number of the

~~TOP SECRET//STLW//HCS//COMINT//ORCON/NOFORN~~

CIA personnel who were read into the PSP were senior CIA managers. [redacted]

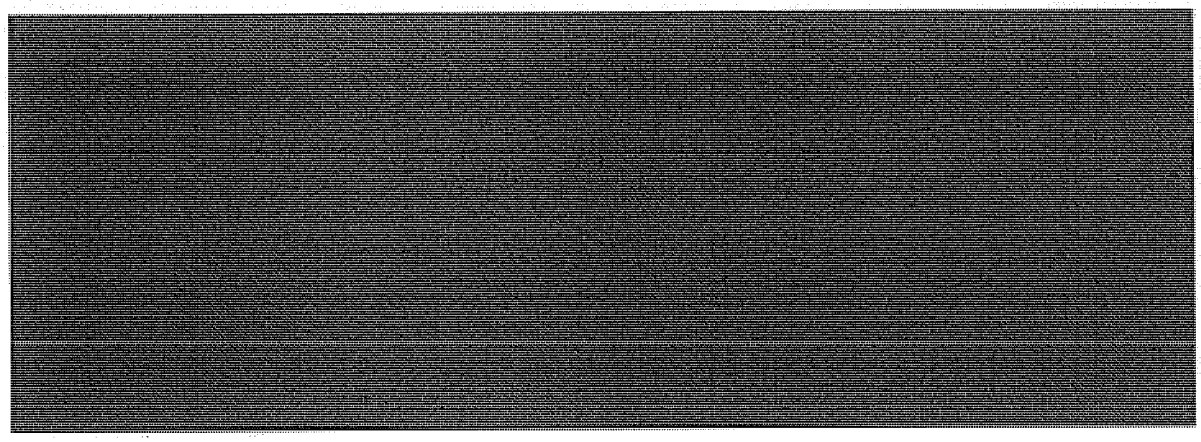
~~(S//NF)~~ [redacted] officials also told us that working-level CIA analysts and targeting officers who were read into the PSP had too many competing priorities, and too many other information sources and analytic tools available to them, to fully utilize PSP. [redacted] officials also told us that much of the PSP reporting was vague or without context, which led analysts and targeting officers to rely more heavily on other information sources and analytic tools, which were more easily accessed and timely than the PSP.

~~(S//NF)~~ CIA officers also told us that the PSP would have been more fully utilized if analysts and targeting officers had obtained a better understanding of the program's capabilities. There was no formal training on the use of the PSP beyond the initial read in to the program. Many CIA officers we interviewed said that the instruction provided in the read-in briefing was not sufficient and that they were surprised and frustrated by the lack of additional guidance. Some officers told us that there was insufficient legal guidance on the use of PSP-derived information. [redacted]

~~(S//NF)~~ The factors that hindered the CIA in making full use of the PSP might have been mitigated if the CIA had designated an individual at an appropriate level of managerial authority, who possessed knowledge of both the PSP and CIA counterterrorism activities, to be responsible and accountable for overseeing CIA participation in the program. [redacted]

~~TOP SECRET//STLW//HCS//COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~



(U) CIA Had Limited Access to Legal Reviews of the President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ There is no indication that personnel from the CIA Office of General Counsel or other CIA components were involved in preparing the legal memorandums supporting the PSP that were produced by the Department of Justice, Office of Legal Counsel (OLC). At the time of the initial authorization of the PSP (4 October 2001), Robert M. McNamara, Jr. was the CIA General Counsel. There is no record that McNamara was ever read into PSP, and he retired from the CIA on 15 November 2001. Acting General Counsel John Rizzo was read into the program on 21 December 2001, but, at that time, he was not provided access to the OLC legal opinions. Rizzo told us that by working through Addington, with whom Rizzo was acquainted, he eventually was allowed to read the OLC legal memorandums at Addington's office in July 2004.

~~(TS//STLW//SI//OC/NF)~~ Scott W. Muller became the CIA General Counsel on 24 October 2002. Although NSA records do not indicate that Muller was read into PSP, during our interview with Muller, he acknowledged having been read into the program and having read the OLC legal memorandums supporting the program. After Jack L. Goldsmith became the Assistant Attorney General for the Office of Legal Counsel in October 2003, the OLC undertook a reassessment of the legal rationale for the PSP. Muller recounted discussions with Deputy Attorney General James B. Comey around March 2004 concerning the legal basis for certain aspects of the program. Muller told us that he shared Comey's concern

Several of the senior CIA managers we interviewed said that, although they were concerned that the PSP operate within legal authorities, they believed that it was important to continue CIA

~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~

participation in the program because CIA analysts and targeters had told them that the program was a useful counterterrorism tool.

~~(S//NF)~~ CIA Officials Sought to Delay Exposure of the President's Surveillance Program by the *New York Times*

~~(S//NF)~~ In October 2004, James Risen, a reporter for *The New York Times*, contacted the CIA Office of Public Affairs seeking an interview with DCI Goss concerning an article the newspaper was planning on the PSP. Senior officials from the CIA, NSA, Office of the Vice President, and the Office of the Secretary of Defense met to discuss a response. On 20 October 2004, DDCI McLaughlin and DCI Chief of Staff Moseman met with the Washington, DC editor of *The New York Times*, Philip Taubman, and Risen. According to a memorandum for the record prepared by Moseman, McLaughlin did not provide any details regarding the PSP or comment on the legal basis for the program, but he stressed that publication of the article would expose, and potentially compromise, effective counterterrorism tools.

~~(S//NF)~~ [redacted] Ultimately, based on assurances from Hayden that he would advise them of inquiries from other news organizations concerning the PSP, Taubman and Risen agreed to hold the article and publish it only when it became apparent that other news organizations were preparing their own stories on the PSP. On 16 December 2005, *The New York Times* published its first article on the PSP: "Bush Lets U.S. Spy on Callers Without Courts." On 17 December 2005, President Bush publicly confirmed in a radio address the existence of the disclosed portion of the PSP.

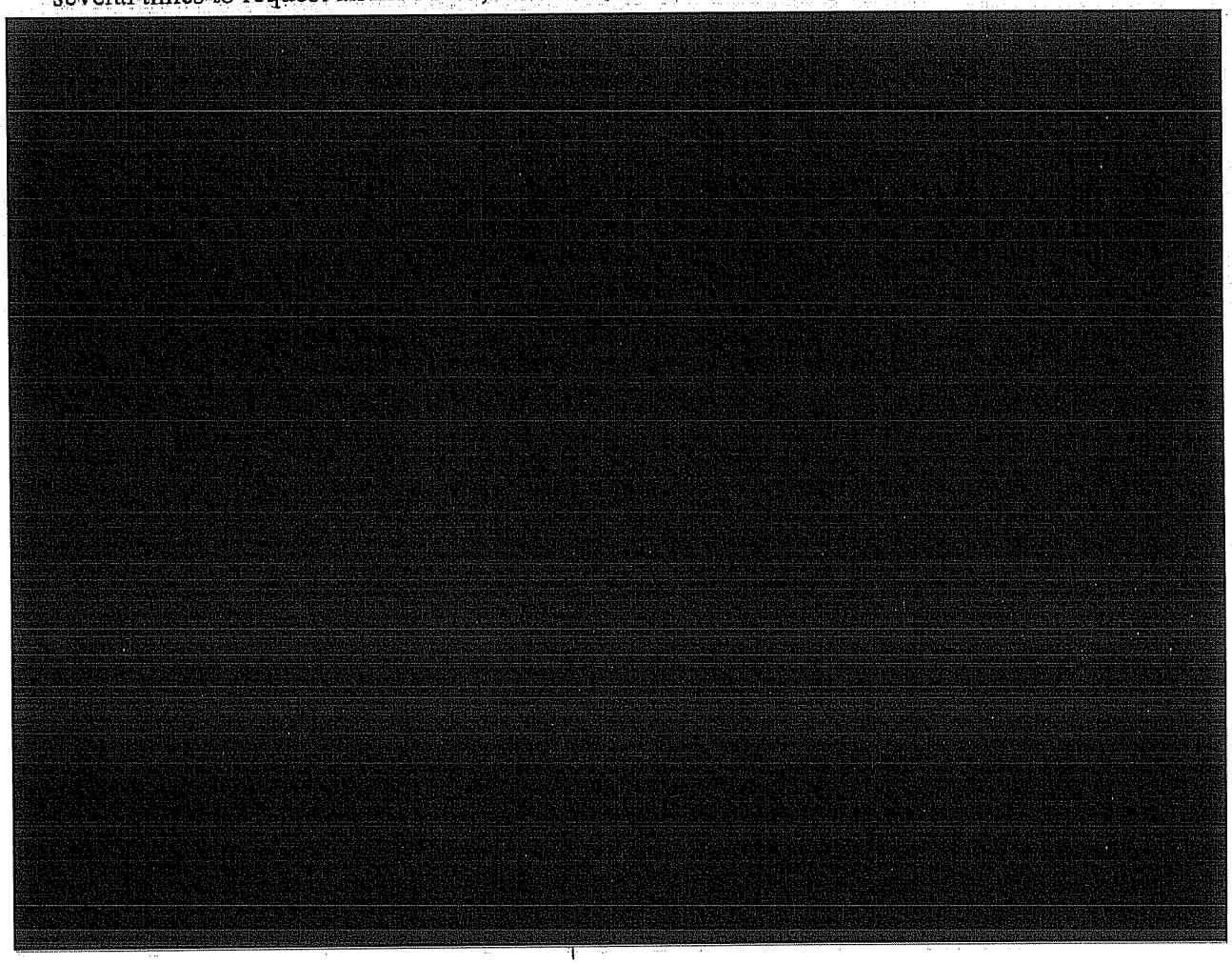
This page intentionally left blank.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

Exhibit A

(U) Methodology

(U//~~FOUO~~) During our review, we conducted 50 interviews of current and former CIA personnel who had been involved with the President's Surveillance Program (PSP). Among the senior CIA officials we interviewed were former Director of the National Security Agency (NSA) and former Director of the CIA (DCIA) Michael V. Hayden, former Director of Central Intelligence (DCI) and former DCIA Porter J. Goss, and former Acting DCI John E. McLaughlin. We contacted former DCI George J. Tenet for an interview. Tenet suggested that we first interview his former Chief of Staff, John H. Moseman, and then contact him if we still had a need to interview him. Following our interview with Moseman, we contacted Tenet's office several times to request an interview, but he did not return our telephone calls.



~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

[redacted]

(U//~~FOUO~~) Management comments were received from Michael V. Hayden; Scott W. Muller; John H. Moseman; the Director, [redacted] and the Chief [redacted] Their comments were considered in preparation of the final report.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

Exhibit B

(U) Threat Assessment Memorandum Concluding Paragraph

[Excerpt from the *Global War Against Terrorism* memorandum dated 10 January 2005.]

~~(TS//STLW//SI//OC/NF)~~ Based on the information available to me from all sources, including the information in this document, it is my estimate that those involved in global terrorism possess both the capability and the intention to undertake further terrorists attacks within the United States, that, if not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of the United States Government. Accordingly, I recommend that, in accordance with the Constitution, you authorize the Secretary of Defense, for the purpose of detection and prevention of terrorist acts within the United States, to employ within the United States the capabilities of the Department of Defense, including but not limited to the signals intelligence capabilities of the National Security Agency, to collect foreign intelligence by electronic surveillance, if such electronic surveillance is intended to:

(a) acquire a communication (including but not limited to a wire communication carried into or out of the United States by cable) for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe such communication originated or terminated outside the United States and a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or any agent of such a group, provided that such group is al Qa'ida, is a group affiliated with al Qa'ida, or is another group that you determine for this purpose is in armed conflict with the United States and poses a threat of hostile action within the United States;

(b) acquire, with respect to a telephony communication, telecommunications dialing-type data, but not the contents of the communication, when (i) at least one party to such communication is outside the United States, (ii) no party to such communication is known to be a citizen of the United States, or (iii) based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are specific and articulable facts giving reason to believe that such communication relates to international terrorism, or activities in preparation therefor; or

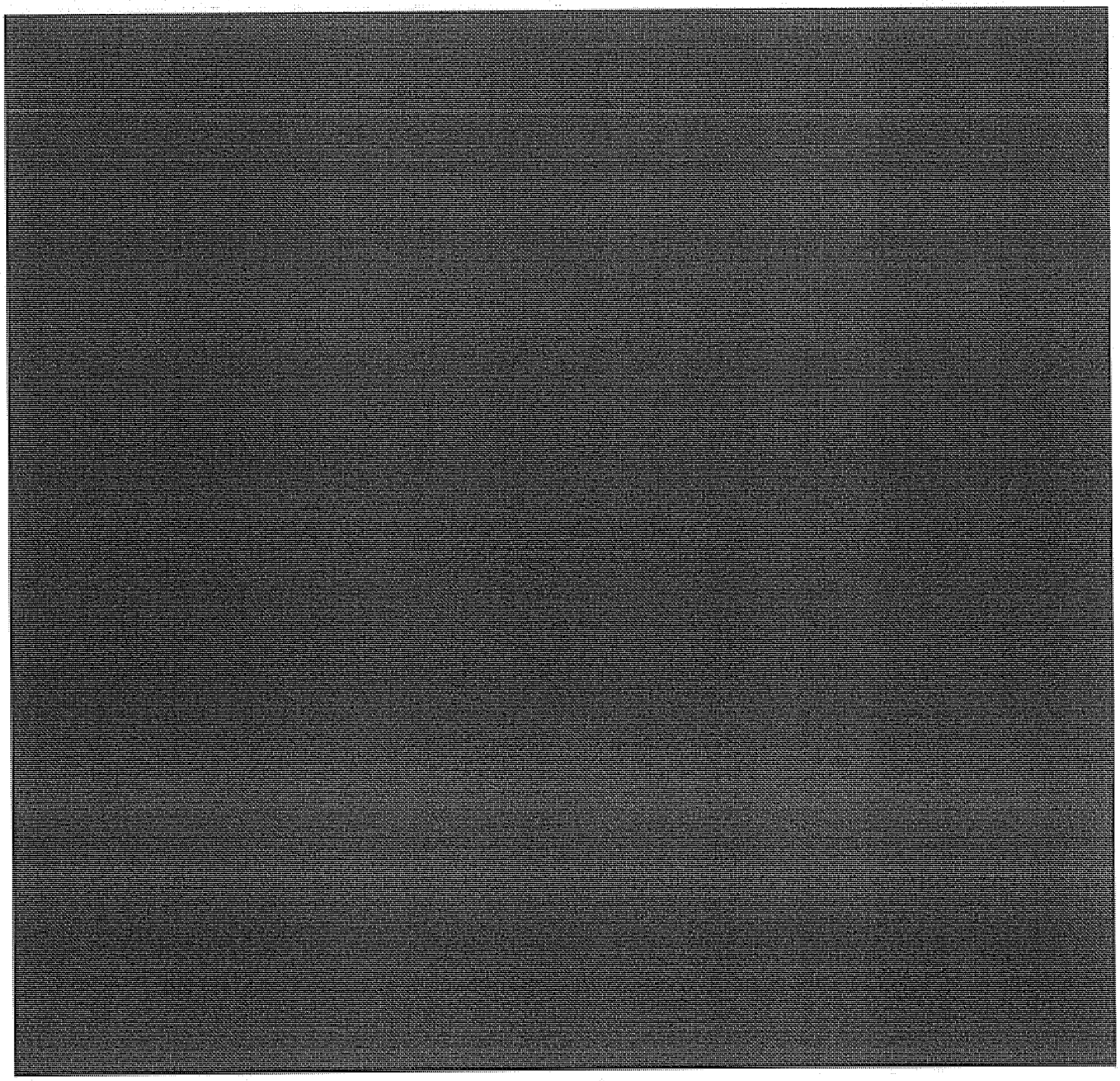
(c) collect, with respect to a non-telephony communication, header/ router/ addressing-type information, but not the contents of the communication, when, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are specific and articulable facts giving reason to believe that a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or any agent of such a group, provided that such group is al Qa'ida, is a group affiliated with al Qa'ida, or is another group that you determine for this purpose is in armed conflict with the United States and poses a threat of hostile action within the United States.

This page intentionally left blank.

~~TOP SECRET//STLW//HCS//COMINT//ORCON/NOFORN~~

Exhibit C

(U) Example of a Link Diagram From August 2002



~~TOP SECRET//STLW//HCS//COMINT//ORCON/NOFORN~~

This page intentionally left blank.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

Exhibit D

(U) Review Team

(U//~~FOUO~~) This report was prepared by the Operations Division, Audit Staff, Office of Inspector General.

[redacted] Division Chief
[redacted] Project Manager
[redacted] Auditor
[redacted] Auditor
[redacted] Auditor

~~This Exhibit is UNCLASSIFIED//FOUO~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

This page intentionally left blank.

~~TOP SECRET//STLW//COMINT//ORCON/NOFORN~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

[redacted]

INSPECTOR GENERAL REPORT

(U) Review of the President's Surveillance Program

ST-09-0002
29 June 2009

~~Derived From: STLW Classification Guide~~
~~Dated: 22 January 2009~~
~~Declassify On: MR~~

~~TOP SECRET//STLW//COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//COMINT//ORCON//NOFORN~~

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts inspections, audits, and investigations. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations; to provide intelligence oversight; to protect against fraud, waste, and mismanagement of resources; and to ensure that NSA/CSS activities are conducted in compliance with the Constitution, laws, executive orders, regulations, and directives. The OIG also serves as ombudsman, assisting all NSA/CSS employees and affiliates, civilian and military.

(U) INSPECTIONS

(U) The inspection function conducts management and program evaluations in the form of organizational and functional reviews, undertaken either as part of the OIG's annual plan or by management request. The inspection team's findings are designed to yield accurate and up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with laws and regulations; the recommendations for corrections or improvements are subject to followup. The inspection office also partners with the Inspectors General of the Service Cryptologic Elements to conduct joint inspections of the consolidated cryptologic facilities.

(U) AUDITS

(U) The internal audit function is designed to provide an independent assessment of programs and organizations. Performance audits evaluate the economy and efficiency of an entity or program, as well as whether program objectives are being met and operations are in compliance with regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) THE OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste and mismanagement. Investigations and Special Inquiries may be undertaken as a result or irregularities that surface during an inspection or audit; or at the initiative of the Inspector General.

~~TOP SECRET//STLW//COMINT//ORCON//NOFORN~~

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

29 June 2009
IG-11051-09

TO: DISTRIBUTION

SUBJECT: (U) Review of President's Surveillance Program (ST-09-0002) — INFORMATION MEMORANDUM

1. (U//~~FOUO~~) This report summarizes our review of the President's Surveillance Program, as mandated by the Foreign Intelligence Surveillance Act Amendments Act of 2008.

2. (U//~~FOUO~~) For additional information, please contact my office on 301-688-6666. We appreciate the courtesy and cooperation extended to our staff throughout the review.

George Ellard

GEORGE ELLARD
Inspector General

DISTRIBUTION:

SID
OGC

(U) EXECUTIVE SUMMARY

(U) OVERVIEW

~~(TS//SI//NF)~~ For over a decade before the terrorist attacks on 11 September 2001, NSA used its SIGINT authorities to provide information in response to Intelligence Community requirements on terrorism targets. In late September 2001, when the Vice President asked the Director of Central Intelligence what more NSA could do with additional authority, NSA's Director identified impediments to enhancing SIGINT collection under existing authorities. He said that in most instances NSA could not collect communications on a wire in the United States without a court order. As a result, NSA's ability to quickly collect and report on a large volume of communications from foreign countries to the United States was impeded by the time-consuming court order approval process. Attempting to obtain court orders for [redacted] foreign telephone numbers and Internet addresses was impractical for collecting terrorist communications with speed and agility.

~~(TS//STLW//SI//OC/NF)~~ Counsel to the Vice President drafted the 4 October 2001 Authorization that established the President's Surveillance Program (PSP), under which NSA could routinely collect on a wire, for counterterrorism purposes, foreign communications originating or terminating in the United States. Under the PSP, NSA did not target communications with both ends in the United States, although some of these communications were incidentally collected.

~~(TS//STLW//SI//OC/NF)~~ The PSP gave NSA a capability to exploit a key vulnerability in terrorist communications.

[redacted]

According to senior NSA leaders, the value of the program was that this SIGINT coverage provided confidence that someone was looking at the seam between foreign and domestic intelligence domains to detect and prevent attacks in the United States.

~~(TS//STLW//SI//OC/NF)~~ NSA's Director said that SIGINT reporting on an extremist linked (b)(1), (b)(3) "probably saved more lives" than any other PSP information and is, therefore, the most important SIGINT success of the PSP. NSA analysis (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~ Knowledge of the Program was strictly limited at the express direction of the White House, and NSA's Director needed White House approval to inform members of Congress about Program activity. Between 25 October 2001 and 17 January 2007, General Michael V. Hayden and Lieutenant General Keith B. Alexander conducted PSP briefings for members of Congress and staff.

~~(TS//STLW//SI//OC/NF)~~ NSA activity conducted under the PSP was authorized by Foreign Intelligence Surveillance Court (FISC) orders by 17 January 2007, when NSA stopped operating under PSP authority. The NSA Office of the Inspector General (OIG) detected no intentional misuse of Program authority.

(U) HIGHLIGHTS

- **(U) PSP establishment, implementation, and product**

~~(TS//STLW//SI//OC/NF)~~ NSA began PSP operations on 6 October 2001. Although the Director of NSA was "comfortable" exercising the new authority and believed that it was lawful, he realized that it would be controversial. Under the PSP, NSA issued over (b)(3) reports. This included (b)(3) reports based on collected metadata, which was defined in the Authorization as "header/router/addressing-type information including telecommunications dialing-type data, but not the contents of the communication." It also included (b)(3) reports based on domestic content collection, which includes words spoken in a telephone conversation or sent in an e-mail (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~ NSA's PSP products, all of which were sent to CIA and FBI, were intended for intelligence purposes to develop investigative leads and were not to be used for judicial purposes.

[redacted] and NSA had no mechanism to track and assess the effectiveness of PSP reporting.

- **(U) Access to legal reviews and program information**

~~(C//NF)~~ NSA's General Counsel and Inspector General were not permitted to read the 2001 DoJ, Office of Legal Counsel opinion on the PSP, but they were given access to draft 2004 Office of Legal Counsel opinions. Knowledge of the PSP was strictly controlled by the White House. Between 4 October 2001 and 17 January 2007, [redacted] people were cleared for access to PSP information.

- [redacted]

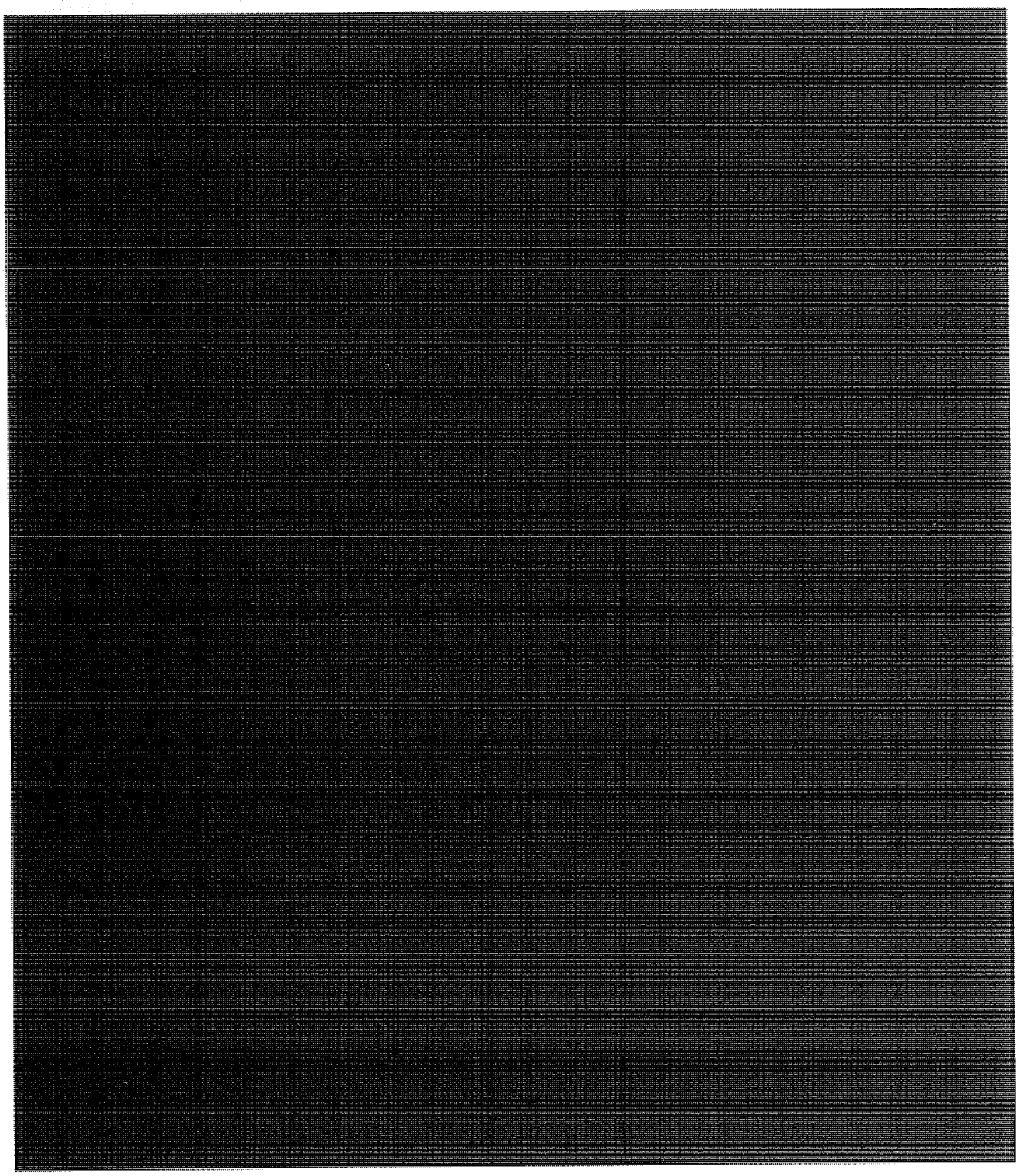
- **(U) NSA-FISC interaction and transition to court orders**

~~(TS//STLW//SI//OC/NF)~~ NSA's PSP-related interaction with the FISC was primarily briefings to presiding judges, beginning in January 2002. Interaction increased when NSA and the DoJ began to transition PSP activities to FISC orders. After parts of the program had been publicly revealed in December 2005, all members of the FISC were briefed. NSA's PSP authorized collection of bulk Internet metadata, telephony business records, and the content of communications transitioned to FISC orders on 14 July 2004, 24 May 2006, and 10 January 2007, respectively.

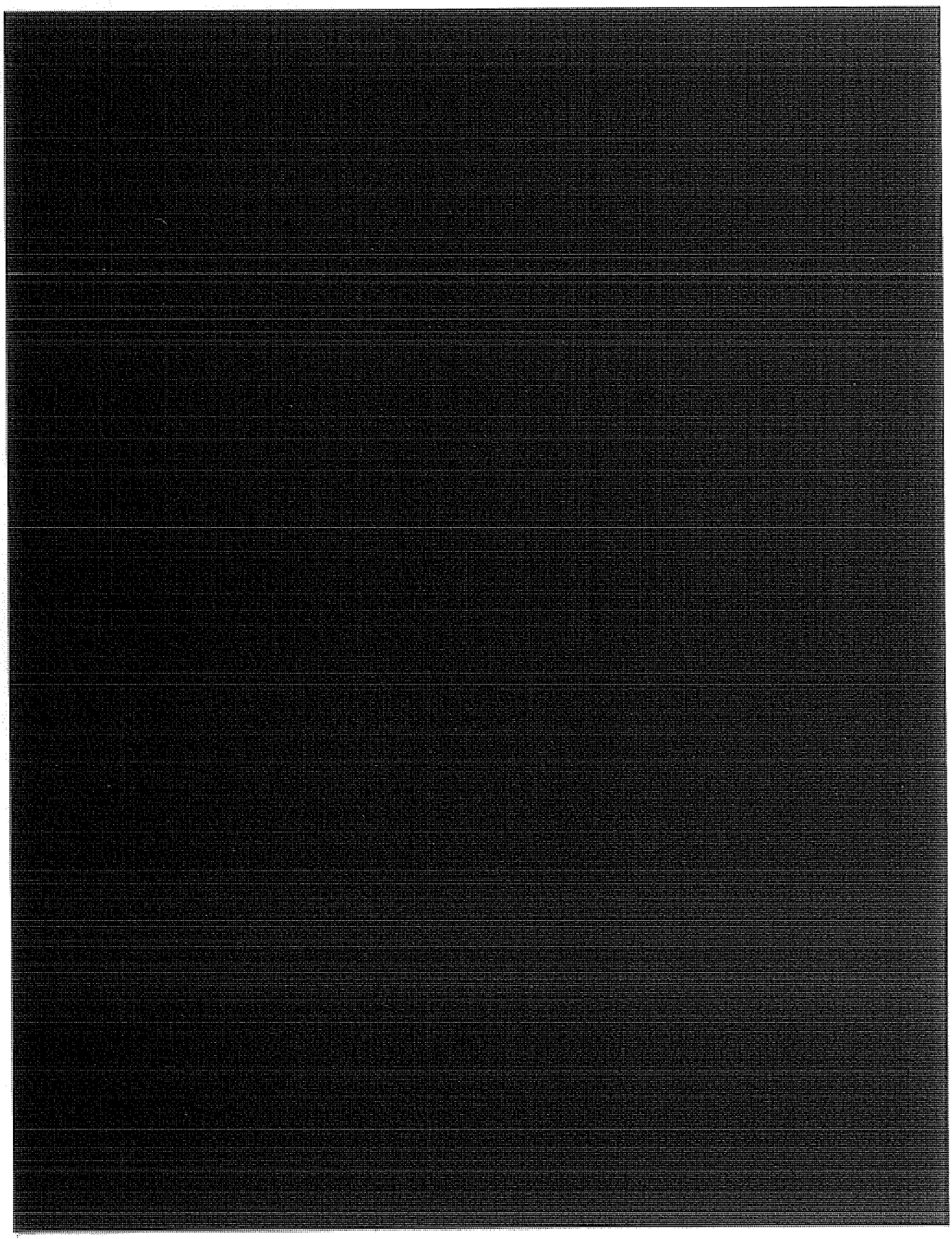
- **(U) Program oversight at NSA**

~~(C//NF)~~ NSA's Office of General Counsel and Signals Intelligence Directorate provided oversight of NSA PSP activities from October 2001 to January 2007. NSA OIG oversight began after the IG was cleared for PSP information in August 2002.

This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.

[redacted]

~~(S//NF)~~ For years before the 11 September 2001 terrorist attacks in the United States, NSA had been using its authorities to focus the United States Signals Intelligence (SIGINT) System on foreign intelligence targets, including terrorism, in response to Intelligence Community requirements. After the attacks, NSA adjusted SIGINT collection, in accordance with its authorities, to counter the terrorist threat within the United States. In late September, the Vice President asked the Director of Central Intelligence (DCI) if NSA could do more to prevent another attack. NSA's Director responded by describing impediments to SIGINT collection of terrorist-related communications to the Vice President. Counsel to the Vice President used the information about impediments to draft the Presidential Authorization that established the PSP.

(U) SIGINT Efforts against Terrorists before 11 September 2001

~~(C//NF)~~ For over a decade before terrorists attacked the United States in September 2001, NSA was applying SIGINT assets against terrorist targets in response to Intelligence Community requirements. The Signals Intelligence Directorate (SID) Counterterrorism (CT) Product Line led these efforts in accordance with SIGINT authorities, which defined what NSA could and could not do against SIGINT targets.

(U) Authorized SIGINT activity in September 2001

(U) NSA was authorized by Executive Order (E.O.) 12333, *United States Intelligence Activities*, 4 December 1981, as amended, to collect, process, and disseminate SIGINT information for foreign intelligence and counterintelligence purposes in accordance with DCI guidance and to support the conduct of military operations under the guidance of the Secretary of Defense. NSA and other Intelligence Community agencies were required by E.O. 12333 to conduct intelligence activities in accordance with U.S. law and other E.O. 12333 provisions.

(U) Both DoD regulation and NSA/Central Security Service (CSS) policy implemented NSA's authorities under E.O. 12333 and specified procedures governing activities that affect U. S. persons (DoD Regulation 5240.1-R, December

1982, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons* and NSA/CSS Policy 1-23, 11 March 2004, *Procedures Governing NSA/CSS Activities that Affect U. S. Persons).*

~~(S//SI//NF)~~ The policy of the U.S. SIGINT System is to collect, retain, and disseminate only foreign communications, which, in September 2001, were defined in NSA's legal compliance procedures (described below) as communications having at least one communicant outside the United States or entirely among foreign powers or between a foreign power and officers or employees of a foreign power. All other communications were considered domestic communications. NSA could not collect communications from a wire in the United States without a court order unless they originated and terminated outside the United States.

~~(S//SI//NF)~~ In 2001, NSA's authority to collect foreign communications included the Director of NSA's authority to approve targeting communications with one communicant in the United States, if technical devices (such as [redacted]) could be employed to limit acquisition of communications to those in which the target is a non-U.S. person located outside the United States, [redacted] or [redacted]

~~(S//SI//NF)~~ NSA's Director could exercise this authority, except when the collection was otherwise regulated, for example, under FISA for communications collected from a wire in the United States.

(U) NSA safeguards to protect U.S. persons' Constitutional rights

(U) The Fourth Amendment to the U.S. Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government.[1] United States Signals Intelligence Directive (USSID) SP0018, *Legal Compliance and Minimization*

---

[1] ~~(C//NF)~~ USSID SP0018 defines a U.S. person as a citizen of the United States, an alien lawfully admitted for permanent residence in the United States, unincorporated groups or associations a substantial number of the members of which constitute either of the first two groups, or corporations incorporated in the United States, including U.S. flag non-governmental aircraft or vessels, but not including those entities openly acknowledged by a foreign government to be directed and controlled by them.

Procedures, 27 July 1993, prescribes policies and minimization procedures and assigns responsibilities to ensure that United States SIGINT System missions and activities are conducted in a manner that safeguards U.S. persons' Constitutional rights. (See Appendix G.)

~~(S//SI//NF)~~ During the course of normal operations, NSA personnel sometimes inadvertently encounter information to, from, or about U.S. persons. When that happens, they must apply standard minimization procedures approved by the Attorney General in accordance with E.O. 12333 and defined in *USSID SP0018*. These procedures implement the constitutional principle of reasonableness by giving different categories of individuals and entities different levels of protection. They ensure that U.S. person information is minimized during collection, processing, dissemination, and retention of SIGINT by, for example, strictly controlling collection with a high risk of encountering U.S. person information and focusing all reporting solely on the activities of foreign entities and persons and their agents.

(U) NSA Director Used Existing Authorities to Enhance SIGINT Collection after Terrorist Attacks

[redacted]

[redacted]

[redacted]

[redacted]

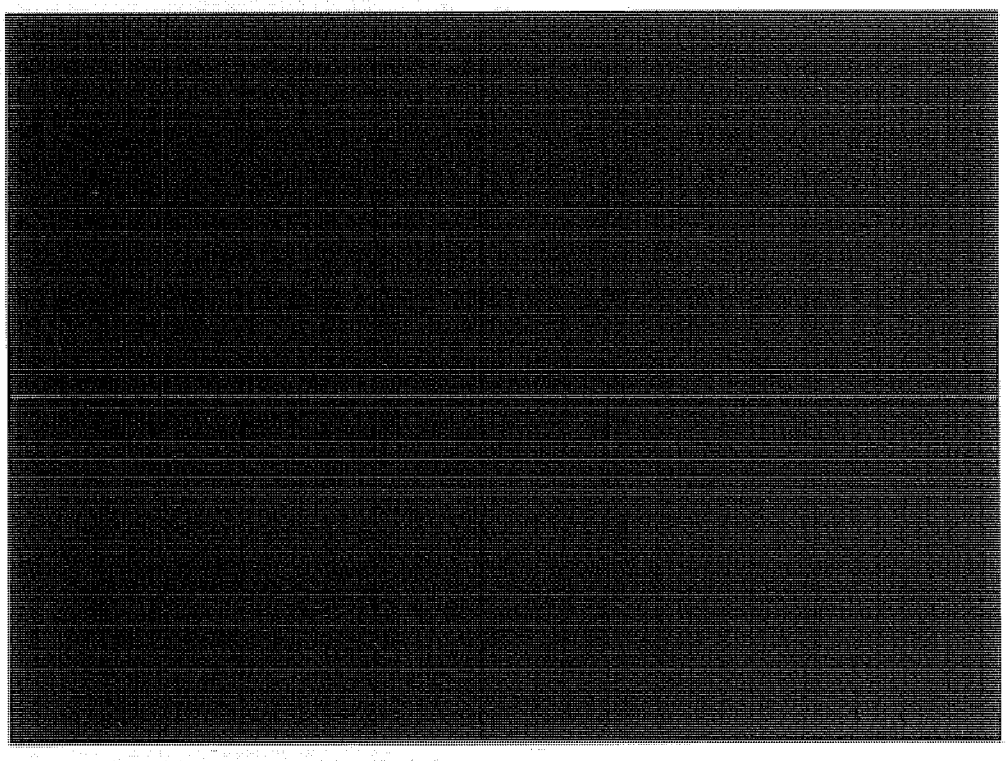
~~(S//NF)~~ In Oval Office Meeting, DCI Explained NSA Director's Decision to Expand Operations under Existing SIGINT Authorities

(U//~~FOUO~~) General Hayden recalled that in late September 2001, he told Mr. Tenet about NSA actions under E.O. 12333 to counter the terrorist threat. Mr. Tenet shared that information with the White House in an Oval Office meeting.

(U//~~FOUO~~) We did not interview Mr. Tenet or White House personnel during this review. We asked the White House to provide documentation of meetings at which General Hayden or NSA employees discussed the PSP or the Terrorist Surveillance Program with the President, Vice President, or White House personnel, but we did not receive a response before this report was published. Therefore, information about the sequence of events leading up to the establishment of the PSP comes from interviews of NSA personnel.

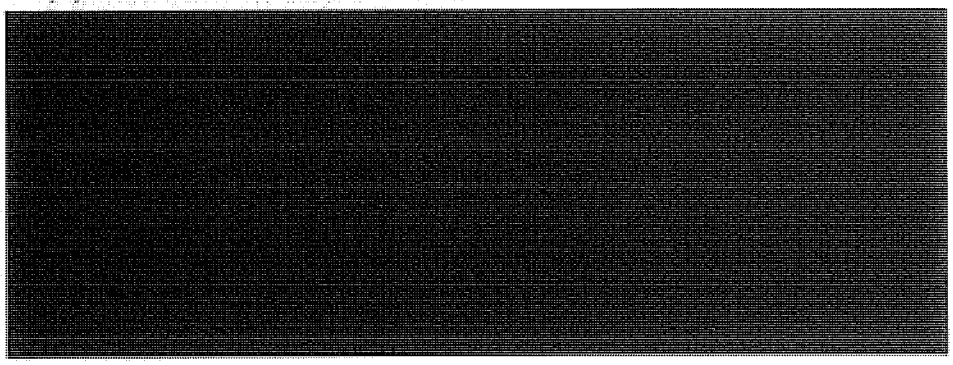
(U) Vice President Asked What Other Authorities NSA Needed

[redacted]



~~(S//NF)~~ NSA Options to Improve SIGINT Collection Could Not Fill Intelligence Gaps on Terrorist Targets

(U) FISA Amendments Considered



~~(S//NF)~~ General Hayden said that, in his professional judgment, NSA could not get the needed collection using the FISA. The process for obtaining court orders was slow, and it involved extensive coordination and separate legal and policy reviews by several agencies. Although an emergency authorization provision permitted 72 hours of surveillance without a court order, it did not allow the government to undertake surveillance immediately. Rather, the Attorney General had to ensure that emergency surveillance would

satisfy the standards articulated in the FISA and be acceptable to the FISC.

[redacted]

~~(S//SI//NF)~~ Under its authorities, NSA had no other options for the timely collection of communications of suspected terrorists when one end of those communications was in the United States and the communications could only be collected from a wire or cable in the United States.

(U//~~FOUO~~) NSA Director Described to the Vice President the Impediments to Improved SIGINT Collection against Terrorist Targets

[redacted]

[4] ~~(TS//SI//NF)~~ According to NSA OGC, DoJ has since agreed with NSA that simply processing communications metadata in this manner does not constitute electronic surveillance under the FISA.

(U//~~FOUO~~) After two additional meetings, the Vice President asked General Hayden to work with his Counsel, David Addington. Because early discussions about expanding NSA authority were not documented, we do not have records of attendees or specific topics discussed at General Hayden's meetings with White House representatives.

III. (U) THE PRESIDENTIAL AUTHORIZATIONS

[redacted]

~~(TS//STLW//SI//OC/NF)~~ Between 4 October 2001 and 8 December 2006, President George W. Bush signed 43 Authorizations, two modifications, and one document described as [redacted] The authorizations were based on the President's determination that after the 11 September 2001 terrorist attacks in the United States, an extraordinary emergency existed for national defense purposes. The Authorization documents contained the terms under which NSA executed special Presidential authority and were titled *Presidential Authorization for Specified Electronic Surveillance Activities during a Limited Period to Detect and Prevent Acts of Terrorism within the United States.* They were addressed to the Secretary of Defense.

(U) SIGINT Activity Permitted under the PSP

[redacted]

[redacted]

(b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~ The authorizations changed over time, first eliminating the possibility that the Authority could be interpreted to permit collection of communications with both ends in the United States and adding an additional qualification that metadata could be collected for communications related to international terrorism or activities in preparation for international terrorism.[7] (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~ Starting in March 2004, the authorizations underwent several adjustments related to DoJ's Office of Legal Counsel's review of the Authority. (b)(1), (b)(3) When these two clarifications were added to the 11 March 2004 and subsequent authorizations, an accompanying statement added that these clarifications had been previously understood and implemented by NSA and that they applied to past and future activities. Al-Qa'ida (also spelled al-Qaeda) was specified as a target for content collection, (b)(1), (b)(3) and NSA's authority to acquire (b)(1), (b)(3) Finally, as a result of a subsequent change, NSA's authority to collect (b)(1), (b)(3) but only fo(b)(1), (b)(3)with (b)(1), (b)(3) thus (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~ The definition of "terrorist groups" within the authorities was also refined, and, for a limited

---

[6]~~(TS//SI//NF)~~ Metadata, as defined by the Authorization, is "header/router/addressing-type information, including telecommunications dialing-type data, but not the contents of the communication."
[7](U) See Appendix B for information about the types of collection permitted.

period in 2004, NSA analysts were permitted to query [redacted]

~~(TS//SI//OC/NF)~~ According to General Hayden, the Authorization, for the most part, did not change the communications that NSA could collect, but did change the location from which the Agency could collect them by permitting collection [redacted] in the United States. Without that authorization, [redacted]

[redacted]

(U) NSA Discussions about the Lawfulness of the Authorization

~~(TS//SI//NF)~~ NSA leaders believed that they could lawfully carry out the President's authorizations. However, they also recognized that the Program would be controversial and politically sensitive. This section describes how key NSA leaders—the Director, the NSA General Counsel, Deputy General Counsel, and Associate General Counsel for

Operations—concluded that the Program was legally defensible.

(U) Director of NSA

~~(TS//SI//NF)~~ Generals Hayden and Alexander stated that they believed the Authorization was lawful.

(U) General Hayden

~~(TS//SI//NF)~~ When asked how he had decided to execute an Authorization that some would consider legally and politically controversial, General Hayden said that NSA's highest ranking lawyers had advised him, collectively and individually, that the Program was lawful under the President's Article II powers. He said that three factors influenced his decision to implement the Authority. First, NSA would do exactly what the Authorization stated and "not one electron or photon more." Second, the Program was simply an expansion of existing NSA collection activities. Third, the periodic renewal of the Authorization would ensure that the threat continued to justify the Program.

~~(TS//SI//NF)~~ General Hayden said that as time passed, he determined that the Program was still needed. Specifically, he and NSA's Deputy Director reviewed the DCI threat memorandum for each reauthorization and judged that the threats continued to justify the Program.

~~(TS//SI//NF)~~ General Hayden said that no one at NSA expressed concerns to him or the NSA IG that the Authorization was not lawful. Most importantly, General Hayden said that no one outside NSA asserted that he should stop the Program. He occasionally heard concerns from members of Congress, but he sensed general support for the Program from those he briefed outside NSA. He emphasized that he did not just "flip through slides" during briefings. He wanted to ensure that attendees understood the Program; consequently, briefings lasted as long as the attendees wanted.

(U) General Alexander

~~(TS//STLW//SI//OC/NF)~~ When Lieutenant General Keith B. Alexander became NSA/CSS Director in mid-2005, some of the more controversial legal questions surrounding the Authorization had been settled, [redacted] the Office of Legal Counsel had

reviewed its initial opinion and determined that the remaining three types of collection were legally supportable.

(U) NSA Office of General Counsel

~~(TS//SI//NF)~~ After the Authorization was signed on 4 October 2001, NSA's highest ranking attorneys, the NSA General Counsel and Deputy General Counsel, as well as the Associate General Counsel for Operations, orally advised General Hayden that the Authorization was legal

(U) General Counsel

~~(TS//SI//NF)~~ After having received the Authorization on 4 October 2001, General Hayden asked NSA General Counsel Robert Deitz if it was lawful. Mr. Deitz said that General Hayden understood that the Attorney General had already certified its legality by signing the Authorization, but General Hayden wanted Mr. Deitz's view. Mr. Deitz said that on 5 October he told General Hayden that he believed the Authorization to be lawful. He added that he emphasized to General Hayden that if this issue were before the Supreme Court, it would likely rule, although not unanimously, that the Authorization was legal.

(U) Associate General Counsel for Operations

~~(TS//SI//NF)~~ On 5 October 2001, the General Counsel consulted the Associate General Counsel for Operations at his home by secure telephone. The Associate General Counsel for Operations was responsible for all legal matters related to NSA SIGINT activities. According to the General Counsel, he had not yet been authorized to tell the Associate General Counsel about the PSP, so he "talked around" it and did not divulge details. The Associate General Counsel was given enough information to assess the lawfulness of the concept described, but records show that he was not officially cleared for the PSP until 11 October 2001. On Tuesday, 9 October, he told Mr. Deitz that he believed the Authorization was lawful, and he began planning for its implementation.

(U) Deputy General Counsel

~~(TS//SI//NF)~~ The Deputy General Counsel was cleared for the PSP on 11 October 2001. He reviewed the Authorization with Mr. Deitz and the Associate General Counsel for Operations and also concluded that it was lawful.

(U) Discussions on Legality

~~(TS//SI//NF)~~ OGC attorneys said that their discussions about the Program's lawfulness took into account the severity of the 11 September attacks and the fear that foreign persons were in the United States planning attacks. The NSA attorneys concluded that the Authorization was lawful. Given the following factors, the General Counsel said the Authorization was constitutional and did not violate FISA.

[redacted]

- ~~(S//NF)~~ FISA was not a realistic means of addressing the terrorist threat inside the United States because the process lacked speed and agility.
- (U//~~FOUO~~) The Authorization was a temporary 30-day grant of authority.
- (U//~~FOUO~~) The statute allowed such an exception, or, to the extent that it did not, it was unconstitutional.

~~(TS//SI//NF)~~ The NSA attorneys determined that the President could issue the Authorization through his authority under Article II of the Constitution to perform warrantless electronic surveillance for foreign intelligence purposes outside and inside the United States. This conclusion, they said, was supported by the concurring opinion in *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), and appellate cases.[8]

~~(TS//SI//NF)~~ The Congressional *Authorization of Use of Military Force* and the canon of constitutional avoidance, which requires a court to attempt to interpret issues so as to avoid constitutional questions, cemented OGC's belief that the President's interpretation of Article II authority had legal merit.

---

[8](U) *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v Buck*, 548 F.2d 871 (9th Cir. 1977); *Zweibon v. Mitchell*, 516 F.2d 594 (DC Cir. 1975); *United States v. Brown* 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974), *cert. denied*, 419 U.S. 881 (1974).

~~(TS//SI//NF)~~ The Associate General Counsel for Operations described his position:

> ~~(TS//SI//NF)~~ Does Congress have the authority to limit Presidential Article II authority in foreign intelligence collection? Given the threat, this was a perfect storm of events—3,000 people killed, airplanes and buildings destroyed by foreign terrorists, an attack in the United States by a foreign terrorist organization. No one knew where the terrorists were or if there were more terrorists, and NSA had a collection capability unable to function because with the FISA, you cannot get [redacted] FISA orders needed to cover what you needed covered at that time to look for the terrorists. You go to the President and tell him that there is a statute that prevents you from doing something from a collection standpoint that may protect the United States from a future attack and that while the country is in danger, I have to adhere with a statute and can't get the amount of warrants I need. Any president is going to say there has got to be a way to do this – a federal law can't let me stand here and watch the country go down the tubes. Does the President have to abide by a statute depriving him of his authority and watch the country go down the tubes? Given the case law of five different circuits with the Supreme Court denying certiorari in two cases, there was good basis for deciding this.

~~(TS//SI//NF)~~ NSA OGC attorneys said that they did not prepare a formal written legal opinion because it was not necessary. The Attorney General had already certified the legality of the Program, and General Hayden had not asked for a written legal opinion. The attorneys also said that they did not have time to prepare a written legal opinion given the pace of operations.

~~(TS//SI//NF)~~ After having concluded that the Authorization was lawful, NSA attorneys believed it was important to ensure that NSA's implementation of the Program complied with the Authorization, that processes were well documented, and that strict controls and due diligence were embedded into the execution of the Program. Recognizing that the legal basis of the Program might become controversial, they said that they wanted to ensure that NSA's execution of the Authority would withstand scrutiny.

This page intentionally left blank.

[redacted]

~~(TS//STLW//SI//OC/NF)~~ NSA PSP operations began on 6 October 2001 and ended on 17 January 2007 and involved the collection, analysis, and reporting of two types of information: metadata and content. NSA assumed that the PSP was temporary and did not immediately formalize processes and procedures for operations, which were quickly set up to provide SIGINT on terrorist targets. As the Authorization continued to be renewed, NSA implemented special procedures to ensure that selectors used for metadata analysis and domestic selectors tasked for content collection were linked to al-Qa'ida, its associates, or international terrorism and that related decisions were documented. NSA did not target communications with both ends in the United States under PSP authority, although some of these communications were incidentally collected, and the OIG found no intentional violations of the Authorization. Over the life of the Program, NSA issued more than [redacted] products based on PSP data. According to senior NSA leaders, the value of the PSP was that SIGINT coverage provided confidence that someone was looking at the seam between the foreign and domestic intelligence domains to detect and prevent attacks in the United States.

(U) NSA Begins PSP Operations

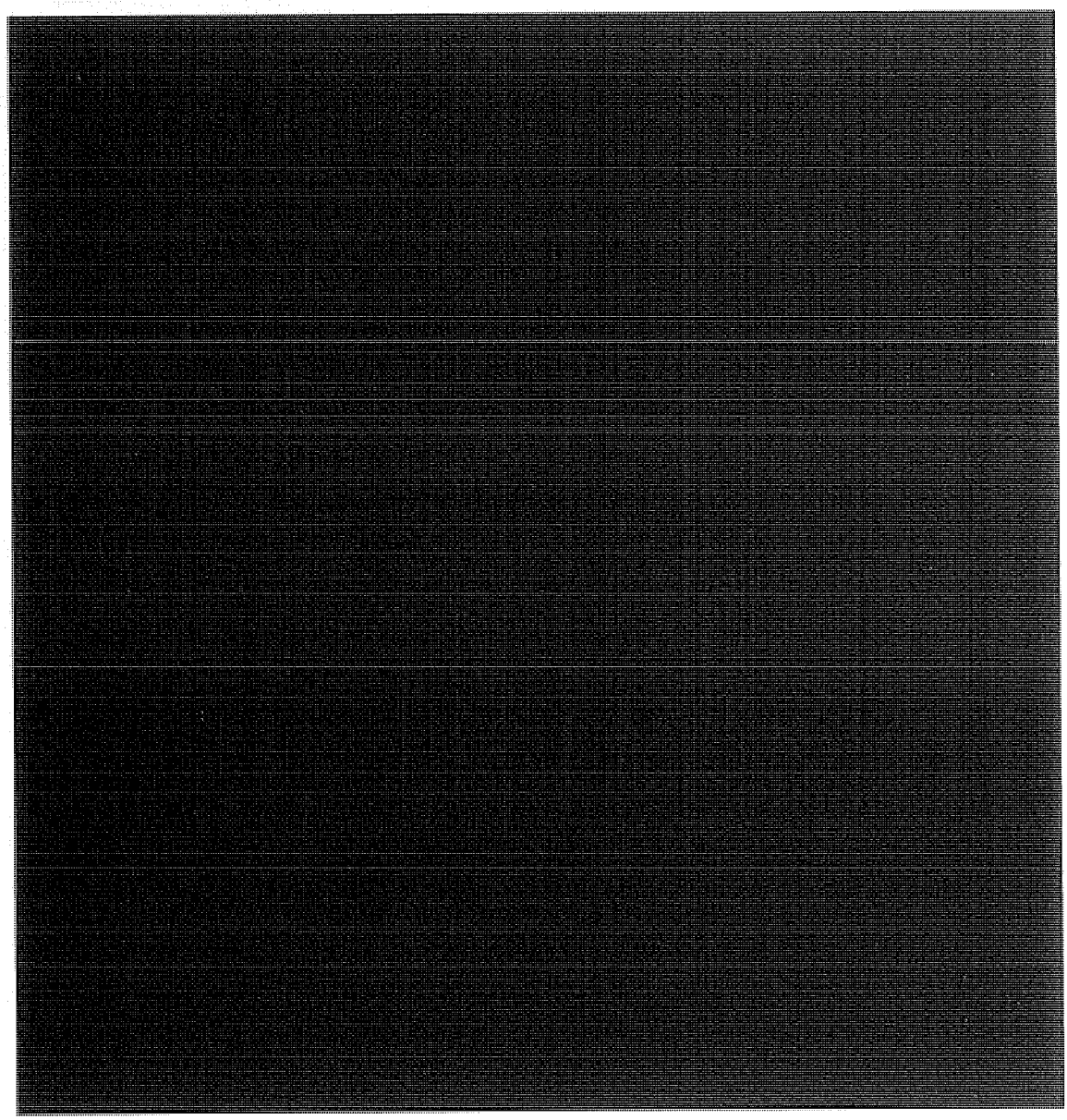
~~(S//NF)~~ On 4 October 2001, General Hayden received the initial Authorization and informed the SIGINT Director and other key personnel.

[redacted]

[redacted]

[9] ~~(S//NF)~~ A permanent cover term, STELLARWIND, was assigned to Program information on 31 October 2001.

[10] ~~(S//NF)~~ [redacted]



~~(TS//SI//NF)~~ **Authorization Renewed**

~~(S//NF)~~ NSA leaders assumed the PSP would be temporary, so they did not establish processes and procedures for a long-term program, and they had plans to cease operations if the Authorization was not renewed. However, the President continued to renew the Authorization, and General Hayden stated that the DCI threat memoranda accompanying each renewal continued to justify the Program.

(U) FISA Authority Still not an Option in 2002

~~(TS//SI//NF)~~ In January 2002, senior NSA leaders still thought that neither the FISA court order process nor the infrastructure associated with FISA collection was suited to large numbers of targets [redacted]

[redacted]

[redacted]

~~(TS//SI//NF)~~ NSA's First Attempt to Obtain FISA Authority on [redacted] Failed.

~~(TS//SI//NF)~~ In September 2002, NSA attempted to obtain FISA authority to collect Internet and electronic wire communications of [redacted] using the standard process for seeking authority on foreign powers and foreign agents. Before preparing an application, NSA submitted a "Memorandum of Justification" to the [redacted][11]

[redacted]

~~(TS//SI//NF)~~ The request was prompted by a CT Product Line staff member, who explained that technical problems delayed NSA's receipt of e-mail collected through FISC orders that the FBI had obtained. [redacted] In one case, an FBI order listed only [redacted] terrorist agents of interest to NSA.

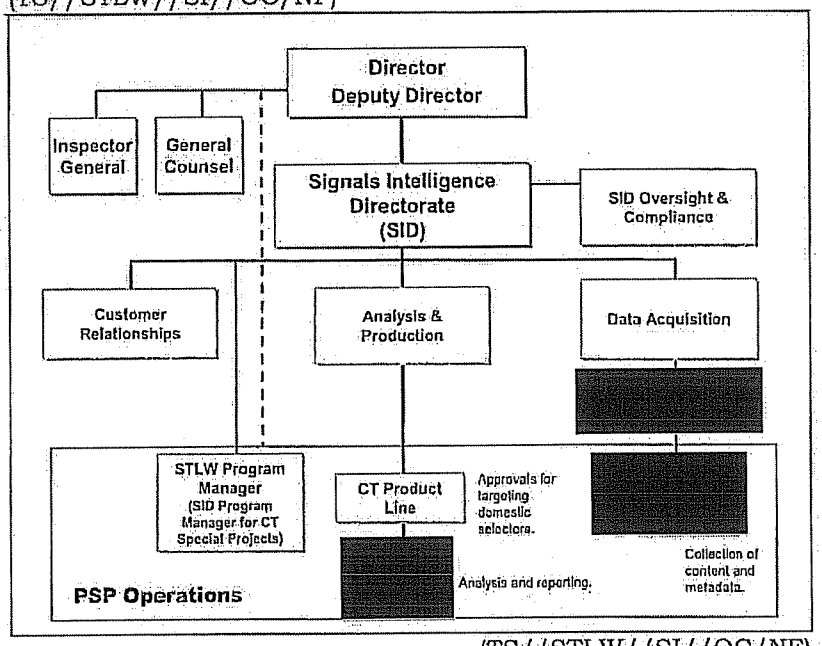
[redacted]

(U) NSA Structure for PSP Operations

[redacted]

(U//~~FOUO~~) NSA Organizational Structure for PSP Activity
November 2004

~~(TS//STLW//SI//OC/NF)~~



~~(TS//STLW//SI//OC/NF)~~

(U) Chain of Command

~~(S//NF)~~ NSA's Director and Deputy Director exercised senior operational control and authority over the Program. According to NSA's Deputy Director, General Hayden handled "downtown" and the Deputy Director managed everything within NSA. The SIGINT Director at the start of the Program stated that once she was confident that the Program had appropriate checks and balances, she left direct management to the Director, Deputy Director, and the OGC. She noted that General Hayden took personal responsibility for the Program and managed it carefully. By 2004, specific roles related to collection, analysis, and reporting had been delegated to the SIGINT Director, who delegated management responsibilities to the Program Manager and mission execution responsibilities to the Chief of the CT Product Line and subordinate leaders.

[redacted]

[redacted]

[redacted]

(U) Coordination with FBI

~~(TS//STLW//SI//OC/NF)~~ On 24 January 2003, NSA, SID, and the FBI agreed to detail FBI personnel working under NSA SIGINT authorities to SID's [redacted] Under the agreement, detailees assisted with terrorism-related SIGINT metadata analysis, identified and disseminated terrorism-related SIGINT information meeting FBI foreign intelligence information needs, and facilitated NSA analyst access to FBI terrorism-related information.

[redacted]

(b)(1), (b)(3)

[redacted]

~~(TS//SI//NF)~~ Minimization Procedures and Additional Controls on PSP Operations[12]

~~(TS//STLW//SI//OC/NF)~~ Management emphasized that the minimization rules required under non-PSP authorities also applied to PSP. The Authorization specifically directed NSA to "minimize the information collected concerning American citizens, to the extent consistent with the effective

[12](U) Internal control, or management control, comprises the plans, methods, and procedures used to meet missions, goals, and objectives. It provides reasonable assurance that an entity is effective and efficient in its operations, reliable in its reporting, and compliant with applicable laws and regulations.

accomplishment of the mission of detection and prevention of acts of terrorism within the United States." NSA complied by applying USSID SP0018 minimization procedures. For example, and as described in the following sections:

- The collection of U.S. person information was minimized by [redacted] (b)(1), (b)(3)

- When analysts encountered U.S. person information, they handled it in accordance with minimization guidance, which included reporting violations or incidents.

- Dissemination of U.S. person information was minimized by requiring pre-release verification that the information was related to counterterrorism and necessary to understand the foreign intelligence or assess its importance.

~~(C//NF)~~ In addition, as PSP operations stabilized and the Authorization continued to be renewed, NSA management designed processes and procedures to implement the Program effectively while ensuring compliance with the Authorization and protecting U.S. person information. By April 2004, formal procedures were in place, many of which were more stringent than those used for non-PSP SIGINT operations. One analyst commented that the PSP "had more documentation than anything else [she] had ever been involved with." Examples of controls, some of which will be explained in more detail in the following sections of this report, include:

- ~~(TS//STLW//SI//OC/NF)~~ Approvals—Shift Coordinators approved foreign and domestic target selectors for metadata analysis. The Chief or Deputy of CT Product Line Chief or the Program Manager approved domestic selectors for content collection under the PSP.

- ~~(TS//STLW//SI//OC/NF)~~ Documentation—RFIs, leads, tasked domestic selectors, and tippers were tracked in the [redacted] Justifications for contact chaining were recorded, and justification packages and approvals for tasking domestic selectors for content collection were formally documented.

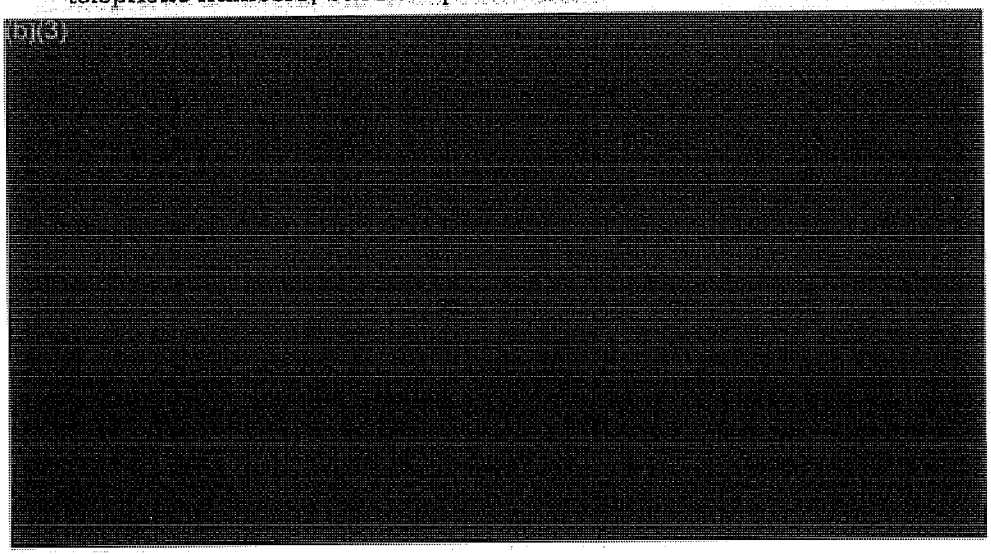
- ~~(TS//SI//NF)~~ Monitoring—Statistics on content tasking and reports were maintained and reviewed by SID, Oversight and Compliance by 2003. A CT Product Line employee stated: "... [N]owhere else did NSA have to report on selectors and how many selectors were rolled off [detasked] and why."

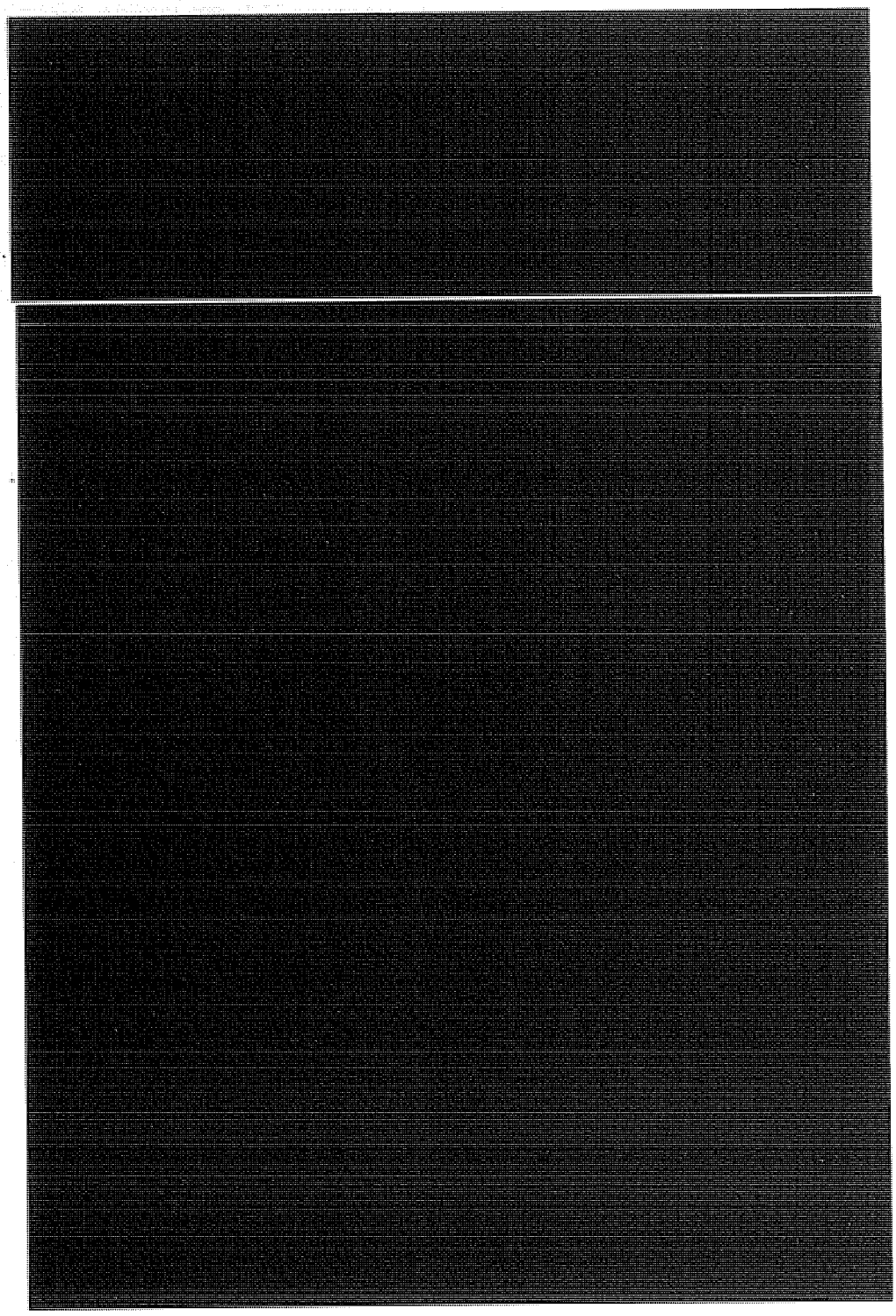
- (U//~~FOUO~~) OGC involvement—Personnel working under PSP authority noted that they had a continuous dialogue with the OGC on what was permissible under the Authorization. The Associate General Counsel for Operations confirmed that the OGC "was involved with the operations people day in and day out."

- (U//~~FOUO~~) Due Diligence Meetings—The PSP Program Manager chaired due-diligence meetings attended by operational, OIG, and OGC personnel. They discussed OIG and OGC reviews and Program challenges, processes, procedures, and documentation.

~~(TS//SI//NF)~~ PSP Operations: Metadata

~~(TS//STLW//SI//OC/NF)~~ The Authorization defines "metadata" as "header/router/addressing-type information, including telecommunications dialing-type data, but not the contents of the communication." For example, e-mail message metadata includes the sender and recipient e-mail addresses. It does not include the subject line or the text of the e-mail, which are considered content. Telephony metadata includes such information as the calling and called telephone numbers, but not spoken words.





~~(TS//SI//NF)~~ Process to Conduct Metadata Analysis

(b)(3)

[redacted]

~~(TS//SI//NF)~~ Standards for Conducting Metadata Analysis

~~(TS//SI//NF)~~ During an OIG review in 2006, the Associate General Counsel for Operations described OGC's standards for complying with the terms of the Authorization when conducting metadata analysis and contact chaining.

~~(TS//SI//NF)~~ To conduct contact chaining under the PSP, the Authorization required that NSA meet one of the following conditions: 1) at least one party to the communication had to be outside the United States, 2) no party to the communication could be known to be a U.S. citizen, or 3) based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there were specific and articulable facts giving reason to believe that the communication relates to international terrorism or activities in preparation therefor. The Associate General Counsel for Operations said that OGC's guidance was more stringent than the Authorization in that the OGC always required that the third condition be met before contact chaining began. Analysts were required to establish a link with designated groups related to international terrorism, al-Qa'ida, or al-Qa'ida affiliates.[14]

~~(S//NF)~~ The Associate General Counsel for Operations said that establishing a link to international terrorist groups or al-Qa'ida and its affiliates met the Authorization's requirement that all activities conducted under the PSP be for the purpose of detecting and preventing terrorist acts within the United States. He explained that because the President had determined that specified international terrorist groups and al-Qa'ida presented a threat within the United States, regardless of where members were located, linking a target selector to such groups established that the collection was for

---

[13](U) Smith v. Maryland, 442 U.S. 735, 742 (1979).

[14]~~(TS//SI//NF)~~ In March and April 2004, authorization language for bulk and Internet metadata and content narrowed from "international terrorism, or activities in preparation therefor," to Al-Qa'ida, a group affiliated with Al-Qa'ida, or another group that the President determined was in armed conflict with the United States and posed a threat of hostile action within the United States.

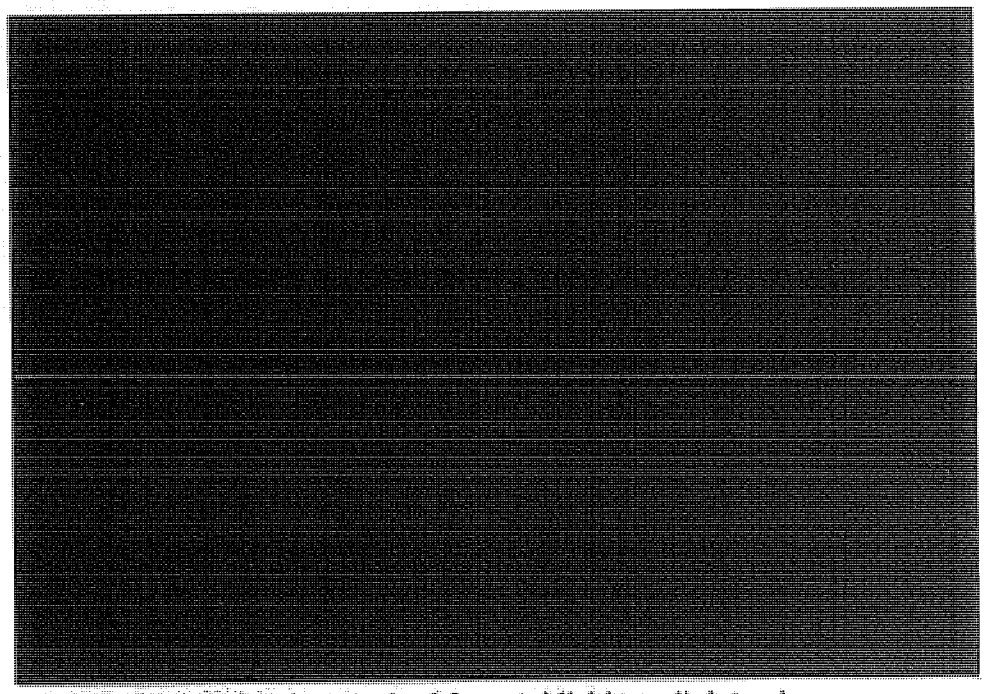
the purpose of detection and prevention of terrorist acts within the United States.

~~(TS//SI//NF)~~ In a 2005 Program memorandum, NSA OGC defined the NSA standard for establishing a link to al-Qa'ida under the PSP. NSA could target selectors when "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe a party to such communication is an agent of al-Qa'ida, or a group affiliated with al-Qa'ida."

> ~~(TS//STLW//SI//OC/NF)~~ Facts giving rise to "reasonable grounds for belief" means reliable facts in NSA's possession, either derived from its signals intelligence activity, or facts provided to NSA by another government department or agency, or facts reliably in the public record (e.g., a newspaper article). Whatever the source of information, the key is that NSA is basing its determination on articulable facts, not on bare assertions made by someone else. We need evidence, rather than conclusions. Thus a mere statement that person X is a member of al Qaeda, without more information, will not suffice as a justification for chaining or for content tasking. Instead we need to know what facts have led NSA, or another agency, or the press, etc., to that conclusion. Focus on the facts and determine whether they lead to a conclusion, rather than accepting someone else's conclusion. If you don't have enough facts to make a determination, ask for them.
>
> ~~(TS//STLW//SI//OC/NF)~~ In addition, the standard does not require certain knowledge, or even necessarily a better than 50/50 chance that the user of a phone or e-mail is a member of al Qaeda or an affiliated organization. It requires only that a reasonable and prudent person exercising good judgment would conclude that there are grounds for believing the thing to be proved. It is not mere hunch or mere suspicion, nor is it proof beyond a reasonable doubt or even a preponderance of the evidence; rather, the standard requires some degree of concrete and articulable evidence or information on which to base a conclusion.

(U) Approvals for Metadata Analysis

[redacted]



~~(TS//SI//NF)~~ If the standard for establishing a link to al-Qa'ida could not be met based solely on the information provided in the RFI or lead, analysts could search NSA and Intelligence Community databases and chain under non-PSP authorities to find additional facts to substantiate the link.

~~(TS//SI//NF)~~ Shift coordinators were not required to approve all alert-list selectors that might have generated [redacted] chaining. One individual, the equivalent of a shift coordinator, managed and monitored the alert process.

~~(TS//SI//NF)~~ When NSA personnel identified erroneous metadata collection, usually caused by technical collection system problems or inappropriate application of the Authorization, minimization procedures required them to report the violation or incident through appropriate channels and to delete the collection from all NSA databases. Early in the Program, NSA reported three violations in which the Authorization was not properly applied and took measures to correct them.

- ~~(TS//STLW//SI//OC/NF)~~ In [redacted] NSA chained on numbers associated with [redacted] In this case, the target was foreign, but there was no link to terrorism.

- ~~(TS//STLW//SI//OC/NF)~~ In [redacted] NSA chained on a domestic telephone number provided by the FBI that was related to a [redacted] investigation. In this case, the target posed a terrorist threat inside the United States, but there was no known link to international terrorism.

- ~~(TS//STLW//SI//OC/NF)~~ In [redacted] NSA chained on metadata based on two telephone numbers provided by FBI related [redacted] While the selectors were associated with international terrorism, [redacted] did not pose a threat of terrorist attacks inside the United States.

~~(TS//SI//NF)~~ Bulk Metadata Needed for Effective Contact Chaining

~~(TS//STLW//SI//OC/NF)~~ Effective contact chaining requires large amounts of metadata, sometimes called bulk metadata, because more data yields more complete chains. [redacted]

~~(TS//STLW//SI//OC/NF)~~ Under PSP authority, NSA obtained a daily average of approximately [redacted] telephony metadata records and an estimated [redacted] Internet metadata records. Metadata obtained under PSP authorities was stored in a protected database, to which only cleared and trained personnel were given access. NSA analysts were able to access and chain through metadata records, but they could view only records associated with an approved foreign intelligence target. This was a small fraction of the metadata available. For example, in August 2006, NSA estimated that only 0.000025 percent or one in every four million archived bulk telephony records was expected to be viewed by trained SIGINT analysts.[15]

---

[15] ~~(TS//SI//NF)~~ This estimate was presented in the August 2006 application for the Business Records Order, the FISC Order that permitted NSA's collection of call detail records. Although this estimate applies to collection and analysis of telephony metadata conducted under the Business Records Order, the same processes and

~~(TS//SI//NF)~~ PSP Operations: Content

~~(TS//STLW//SI//OC/NF)~~ (b)(3) [redacted] PSP content operations involved three separate activities: tasking selectors for content collection, collecting the content of communications associated with tasked selectors, and analyzing the content collected. To comply with the Authorization, NSA management combined standard minimization procedures and specially designed procedures to task domestic selectors, collect the resulting communications, and analyze and report the foreign intelligence they contained. Over the life of the Program, NSA tasked approximately (b)(1), [redacted] foreign and domestic selectors for content collection.

~~(TS//SI//NF)~~ Tasking Selectors for Content Collection

~~(TS//STLW//SI//OC/NF)~~ "Tasking" is the direct levying of SIGINT collection requirements on designated collectors. Analysts must task selectors to obtain a target's communications.

~~(TS//STLW//SI//OC/NF)~~ Under the PSP, (b)(1), (b)(3) [redacted] Before NSA personnel tasked target selectors for PSP content collection, the Authorization required that target selectors comply with two criteria. First, they had to determine that "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe a party to such communication is an agent of al Qa'ida, or a group affiliated with al-Qa'ida," as described in guidance issued by OGC in 2005. Second, the purpose of the collection had to be the prevention and detection of terrorist attacks in the United States. The OGC provided the same guidance for tasking selectors for content collection as it had for contact chaining. Specifically, because the President had determined that al-Qa'ida presented a threat within the United States, regardless of where its members were located, linking a target selector to designated international terrorist groups or al-Qa'ida and its affiliates, established that the collection was for the purpose of detection and prevention of terrorist acts within the United States.

---

techniques were used under the PSP, making this a reasonable comparison. This estimate was based on data available in August 2006 and cannot be replicated.

~~(TS//SI//NF)~~ Approvals to Task Domestic Selectors for Content Collection

~~(TS//SI//NF)~~ NSA analysts determined whether foreign selectors met the Authorization criteria and tasked them without further approval. However, because NSA leadership considered selectors located in the United States to be extremely sensitive, the associated tasking process required extra documentation, reviews, and approvals than foreign selector tasking under the PSP.

[redacted]

[redacted]

[16](U) From 2005 to 2007, SID, Analysis and Production leadership titles changed. The Primary Production Center Manager became the primary approval authority for tasking packages.

[redacted]

~~(TS//SI//NF)~~ **Most Selectors Tasked for Content Collection Were Foreign.**

[redacted]

~~(TS//STLW//SI//OC/NF)~~ In 2008, NSA reported to a member of Congress that [redacted] domestic telephone numbers and [redacted] domestic Internet addresses were tasked for PSP content collection from October 2001 to January 2007. Domestic selectors were located in the United States and associated with al-Qa'ida or international terrorism and were not necessarily used by U.S. citizens. In a 2008 Attorney General Certification, NSA reported that [redacted] foreign telephone numbers and in excess of [redacted] foreign Internet addresses had been targeted from October 2001 through December 2006, which spans all but one month of the Program. NSA could not precisely estimate the number of

foreign Internet addresses targeted because the tools used by analysts before September 2005 did not accurately account for the number of individual addresses targeted.

~~(TS//SI//NF)~~ In 2006, the OIG Found that Justifications for Tasking Domestic Selectors Met Authorization Criteria.

~~(TS//STLW//SI//OC/NF)~~ During a 2006 review, the OIG found that all items in a randomly selected sample of tasked domestic selectors met Authorization criteria. Based on a statistically valid sampling methodology, the OIG was able to conclude with 95 percent confidence that 95 percent or more of domestic selectors tasked for PSP content collection could be linked to al-Qa'ida, its associates, or international terrorist threats inside the United States. Justification packages for all sample items tested were supported by one or more of the following types of information:

[redacted]

- Information associated with or obtained through FBI investigations.

(U) Process to Task Selectors

[redacted]

[redacted]

~~(TS//SI//NF)~~ In 2005, the OIG found that the largely manual process to task and detask selectors for content collection was unreliable. Specifically, the OIG found [redacted] errors when comparing records of domestic telephone numbers and Internet identifiers approved for PSP content collection as of November 2004 with those actually on collection. The errors consisted of selectors that had not been removed from collection after being detasked, had not been put on collection after having been approved, had been put on collection because of a typographical error, or had not been accurately recorded in the [redacted] In response to the OIG finding, management took immediate steps to correct the errors and set up a process to reconcile approved tasked selectors with selectors actually on collection.

~~(TS//SI//NF)~~ Collecting the Content of Communications

(U//~~FOUO~~) Collection refers to the process of obtaining communications after selectors associated with intelligence targets are tasked for collection at designated sites. Data collected under the PSP was stored in protected partitions in NSA databases. Access to the partitions was restricted to PSP-cleared personnel.

~~(TS//SI//NF)~~ The Authorization required that a collected communication originate or terminate outside the United States. NSA did not intentionally collect domestic communications under the PSP. [redacted] and the CT Product Line to ensure that collected data was as intended and authorized. According to PSP program officials, NSA's [redacted] Its purpose was to collect international communications. However, management stated that:

> There are no readily available technical solutions within the [redacted] to guarantee that no [domestic] calls will be collected. Issues of this kind inevitably arise from time to time in other SIGINT operations, as foreseen by Executive Order 12333, and are thus not peculiar to [the PSP].

~~(S//NF)~~ The Program Management Office identified four ways that NSA might have unintentionally collected non-target data:

- A target could have been correctly tasked using valid selectors, but, in addition to collecting the desired target communications, non-target communications were inadvertently collected.
- A valid target selector could have generated target-specific collection that ultimately proved the target not to be related to al-Qa'ida.
- A technical, human, or procedural error in the target identification or tasking process could have resulted in unintentional collection of communications not related to al-Qa'ida.
- Technical collection system problems could have resulted in unintentional collection of non-al-Qa'ida related targets, even when all steps in the target identification and tasking process had been properly executed.

~~(S//NF)~~ Over the life of the Program, NSA reported [redacted] incidents of unintentional collection of domestic communications and [redacted] incidents in which the wrong selector had been tasked. (See Appendix F for details.) In those cases, personnel followed USSID SP0018 procedures and were given detailed instructions to report the violations or incidents, adjust tasking, and delete collection records from NSA and other databases.

~~(TS//SI//NF)~~ Analyzing the Content of Collected Communications

~~(TS//SI//NF)~~ Analysis of content collected under the PSP involved the same practices and techniques used in non-PSP operations. One NSA manager described the PSP as "just one more tool in the analysts' tool kit." [redacted] Collected communications were then transcribed, if necessary, and processed to make them useful for intelligence analysis and reporting. Analysis included not only listening to or reading the contents of a communication, but drawing on target knowledge, coordinating and collaborating with other analysts, and integrating collateral information, metadata, and information from databases and published intelligence

reports to determine whether the communications included foreign intelligence that was timely, unique, actionable, and reportable.

[redacted]

---

[17](U//~~FOUO~~) A serialized report is a formatted intelligence product produced pursuant to USSID CR1400 that has a reference serial number, contains foreign intelligence information derived from SIGINT, and goes to approved users of intelligence.

[18](~~TS//STLW//SI//OC/NF~~) NSA issued [redacted] additional reports between 17 January 2007 and December 2008 that were based on analysis of data previously collected under PSP authority.

[redacted]

~~(TS//SI//NF)~~ Metadata Analysis Reports (Tippers)

~~(TS//STLW//SI//OC/NF)~~ Reports based on metadata analysis were referred to as "tippers." [redacted]

[redacted] b1, b3, b7E

~~(TS//STLW//SI//OC/NF)~~ NSA retained documentation of the analysis, supporting customer request or lead information, and a description of the link to terrorism for tippers based on PSP collection. Documentation of analysis was not retained unless a tipper was written. Counterterrorism personnel updated information in a computer tracking system to reflect the disposition of all metadata analysis requests. From October 2001 through January 2007, NSA issued [redacted] tippers to FBI and CIA: b1, b3, b7E

- [redacted] tippers were based on Internet metadata analysis.
- [redacted] tippers were based on telephony metadata analysis when telephone numbers had only direct contact (one degree of separation) with a known terrorist as defined by the Authorization. b1, b3, b7E

- [redacted] tippers were based on more detailed telephony metadata analysis that included contacts with two degrees of separation from known terrorists. b1, b3, b7E
- [redacted] tippers were based on telephony and Internet metadata analysis.

~~(TS//SI//NF)~~ Content Reports

~~(TS//STLW//SI//OC/NF)~~ PSP content reports contained NSA's analysis of communications [redacted] b1, b3, b7E

(U//~~FOUO~~) Protection of U.S. Person Information in Reporting

~~(TS//SI//NF)~~ Before sending PSP reports to customers, NSA removed unnecessary U.S. person information, as required by minimization procedures in *USSID SP0018*. The CT Product Line reviewed PSP reports to ensure that they had been written in accordance with these procedures. SID's Oversight and Compliance office then reviewed PSP reports containing U.S. person information. Oversight and Compliance personnel reviewed U.S. person information in reports, determined if it was necessary to understand the foreign intelligence in the reports, and submitted recommendations for the inclusion of U.S. person information to SID, Chief of Information Sharing Services for final approval. For example, if an individual's name was not necessary to understand the foreign intelligence in the report, the name was deleted or changed to "a U.S. person."

~~(TS//SI//NF)~~ Oversight and Compliance did not review tippers based on metadata analysis. When NSA began to issue tippers based on the content of communications, SID adapted its procedures for the dissemination of U.S. person information. Additional Oversight and Compliance personnel were cleared for the Program to assist with reviews. They gave PSP and other terrorism reporting priority for review over other Agency reporting.

(U) Use of SIGINT Product

~~(TS//SI//NF)~~ As NSA's primary customers for PSP information, [redacted] All products included this statement:

> This information is provided only for intelligence purposes in an effort to develop potential investigative leads. It cannot be used in court proceedings, subpoenas, or for other legal or judicial purposes.

(U//~~FOUO~~) Value of the PSP

~~(TS//SI//NF)~~ Referring to portions of the PSP in 2005, General Hayden said there were probably no communications more important to NSA efforts to defend the nation than those involving al-Qa'ida. NSA collected communications when one end was inside the United States and one end was associated with al-Qa'ida or international terrorism in order to detect and prevent attacks inside the United States. General Hayden stated that "the program in this regard has been successful." During the May 2006 Senate hearing on his nomination to be CIA Director, General Hayden said that, had the PSP been in place before the September 2001 attacks, hijackers Khalid Almihdhar and Nawaf Alhazmi almost certainly would have been identified and located.

~~(TS//SI//NF)~~ In May 2009, General Hayden told us that the value of the Program was in knowing that NSA SIGINT activities under the PSP covered an important "quadrant" (terrorist communications between foreign countries and the United States). This coverage provided confidence that there were "not additional terrorist cells in the United States." NSA's Deputy Director, who was the SID Deputy Director for Analysis and Production on 11 September 2001, echoed

General Hayden's comment: "The value of the PSP was in the confidence it provided that someone was looking at the seam between the foreign and domestic intelligence domains."

~~(TS//SI//NF)~~ The former SID Deputy Director for Data Acquisition said that the possibility of a large terrorist presence in the United States [redacted] The PSP gave NSA a capability to exploit a key vulnerability in terrorists' communications: [redacted] With PSP authority, NSA could collect communications between [redacted] al-Qa'ida [redacted]

~~(TS//STLW//SI//OC/NF)~~ Current NSA Director General Alexander cited SIGINT reporting on [redacted] as the most important SIGINT success of the PSP. NSA analysis of PSP metadata and content collection placed [redacted], General Alexander said, "probably saved more lives" than any other PSP information produced by NSA because the information [redacted] b1, b3, b6, b7C, b7E

~~(TS//SI//NF)~~ From an operational standpoint, the PSP enabled NSA to:

- Support customers
- Provide SIGINT that contributed to customers' investigative work

[redacted]

(U//~~FOUO~~) Support to Customers

~~(TS//SI//NF)~~ From April 2002 to January 2007, NSA responded to [redacted] and more than [redacted] from FBI. These numbers do not account for requests submitted before NSA began to use an automated tracking system in April 2002.

~~(TS//SI//NF)~~ Based on information obtained under PSP authority, NSA sent [redacted]

and FBI. In the early days of the Program, the FBI said that the large number of tippers from NSA was causing them unnecessary work because agents treated each tipper as a lead requiring action. General Hayden said that NSA's intention was that SIGINT information be added to FBI's knowledge base, not that the FBI act on each piece of information. When NSA realized that it was sending too much data to the FBI, the Agency made appropriate adjustments.

~~(U//FOUO)~~ PSP Reporting Contributed to Customers' Investigative Work.

~~(TS//STLW//SI//OC/NF)~~ [redacted] For example, an FBI briefing dated 4 May 2006 stated that "STELLARWIND continues to provide timely and carefully vetted intelligence to support FBI's investigations in connection with [redacted] operations]."

~~(TS//STLW//SI//OC/NF)~~ [redacted] FBI did not routinely provide feedback on NSA reporting under the PSP, and NSA had no mechanism to track and assess the effectiveness of SIGINT reporting in general or PSP reporting in particular.[19] Tracking PSP contributions was also difficult because customers did not know that [redacted] General Hayden noted that success stories decreased over time as intelligence became more integrated and it became more difficult to attribute success to any one activity.

~~(TS//STLW//SI//OC/NF)~~ The Program Management Office provided the following examples of PSP reporting that helped redirect FBI resources [redacted] viewed as vulnerable to terrorism targeting. The examples also include cases in which NSA provided reporting that contributed to FBI investigations, FBI confidential human sources, FISA warrants, arrests, and convictions.

---

[19] ~~(C//NF)~~ In July 2007, SID initiated a formal effort to assess the effectiveness of its CT efforts. By the fall of 2007, that effort was struggling.

(U) Case Name	(U) PSP Contribution
(b)(1), (b)(3)	

b1, b3, b6, b7C, b7D, b7E

(U) Case Name	(U) PSP Contribution
(b)(1); (b)(3)	

b1,
b3,
b6,
b7C,
b7E

(U) Case Name	(U) PSP Contribution
(b)(1), (b)(3)	

b1, b3, b6, b7C, b7E

(U) PSP Information	(U) Description of SIGINT Reporting
[redacted]	

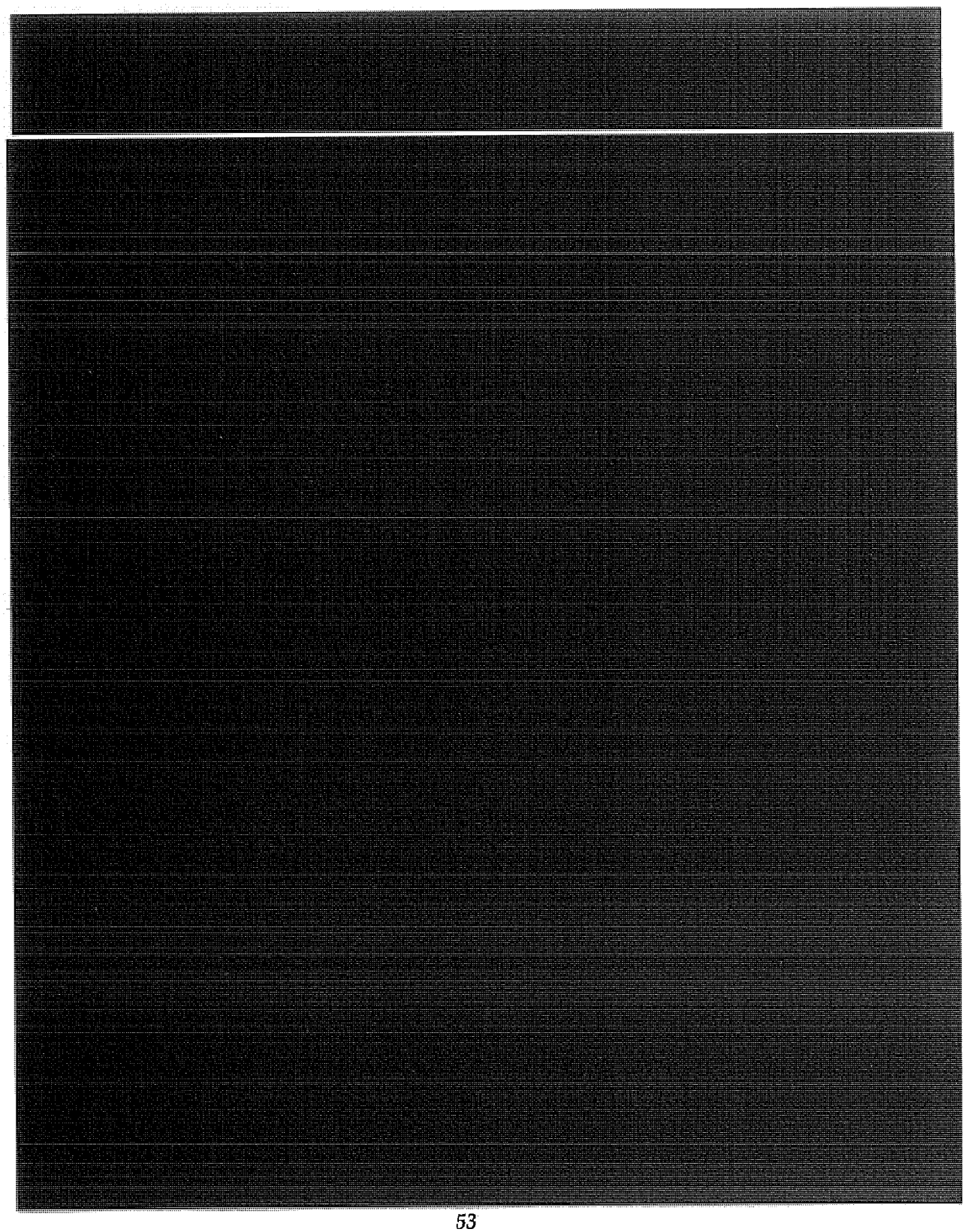
(U) PSP Information	(U) Description of SIGINT Reporting
[redacted]	

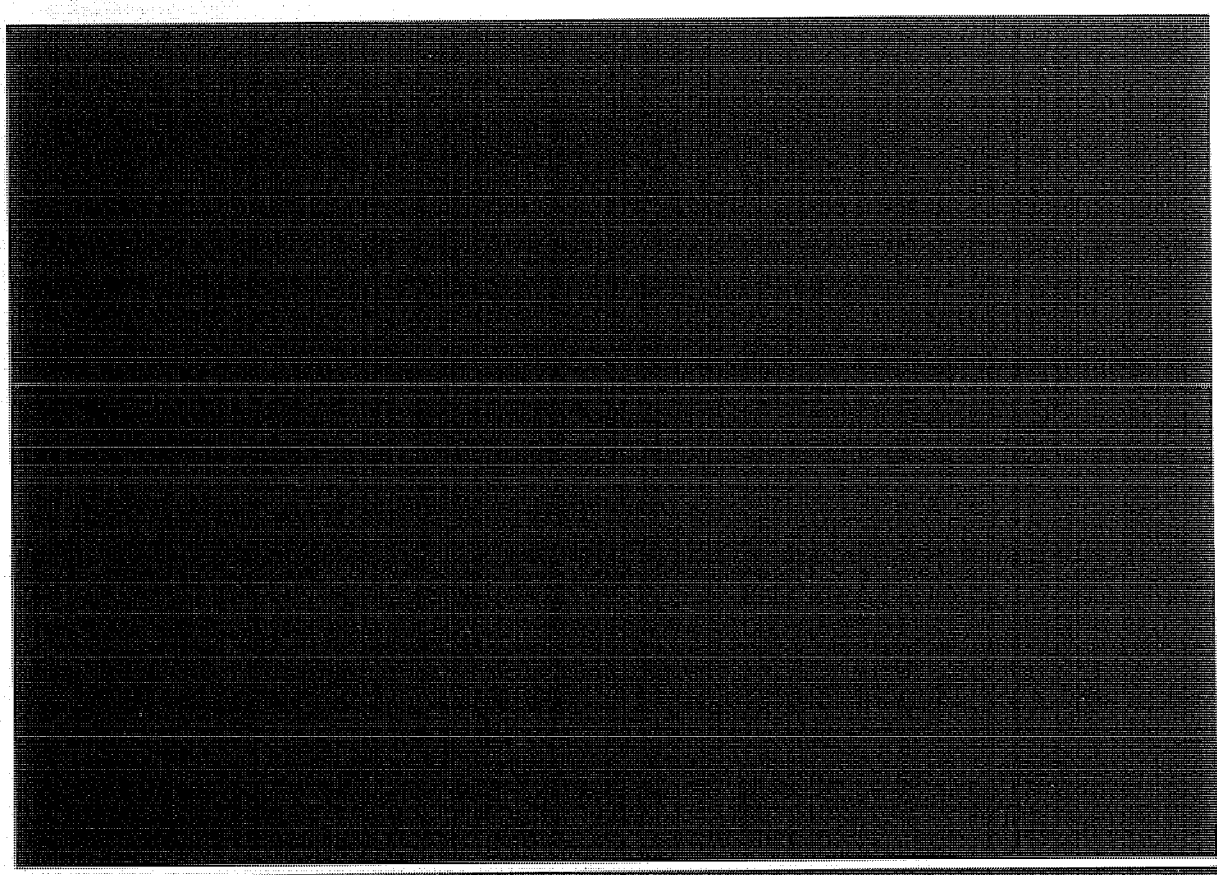
(U) PSP Information	(U) Description of SIGINT Reporting
[redacted]	

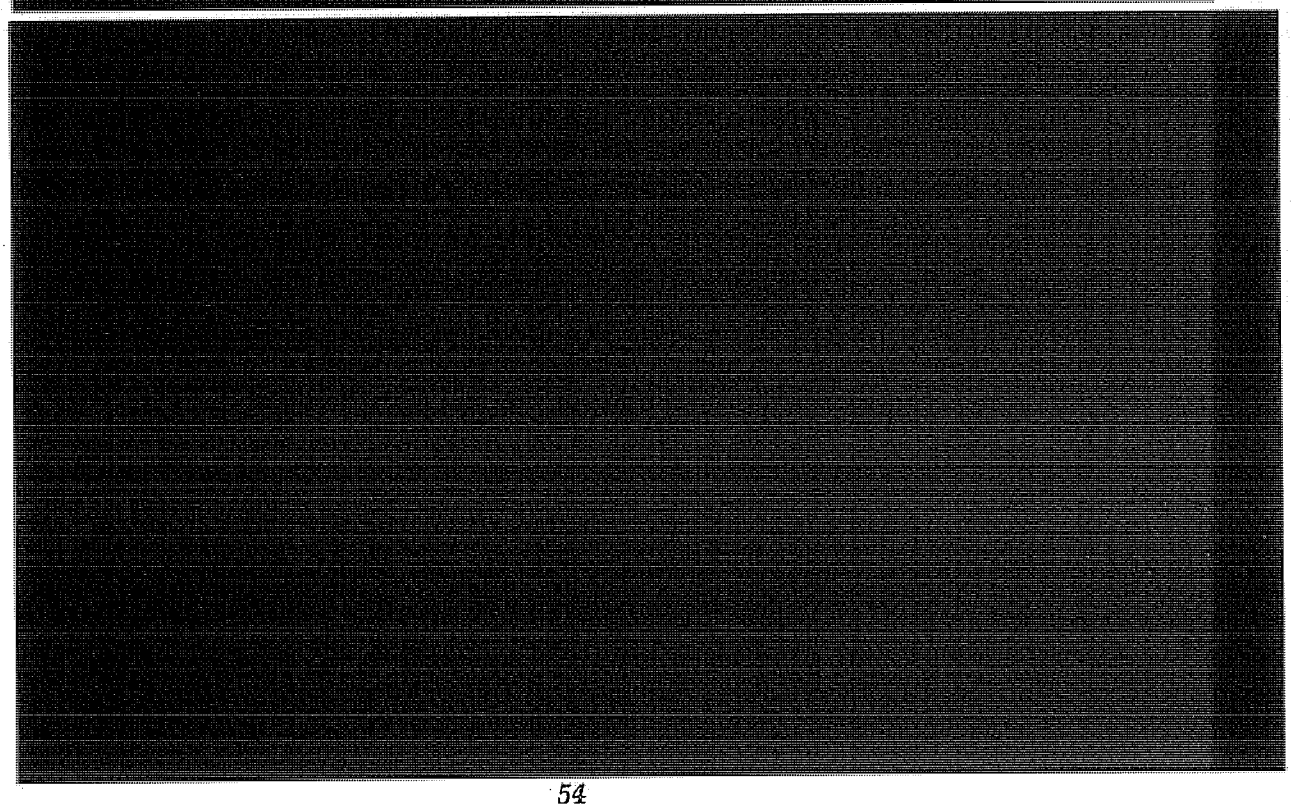
b1,
b3,
b6,
b7C,
b7E

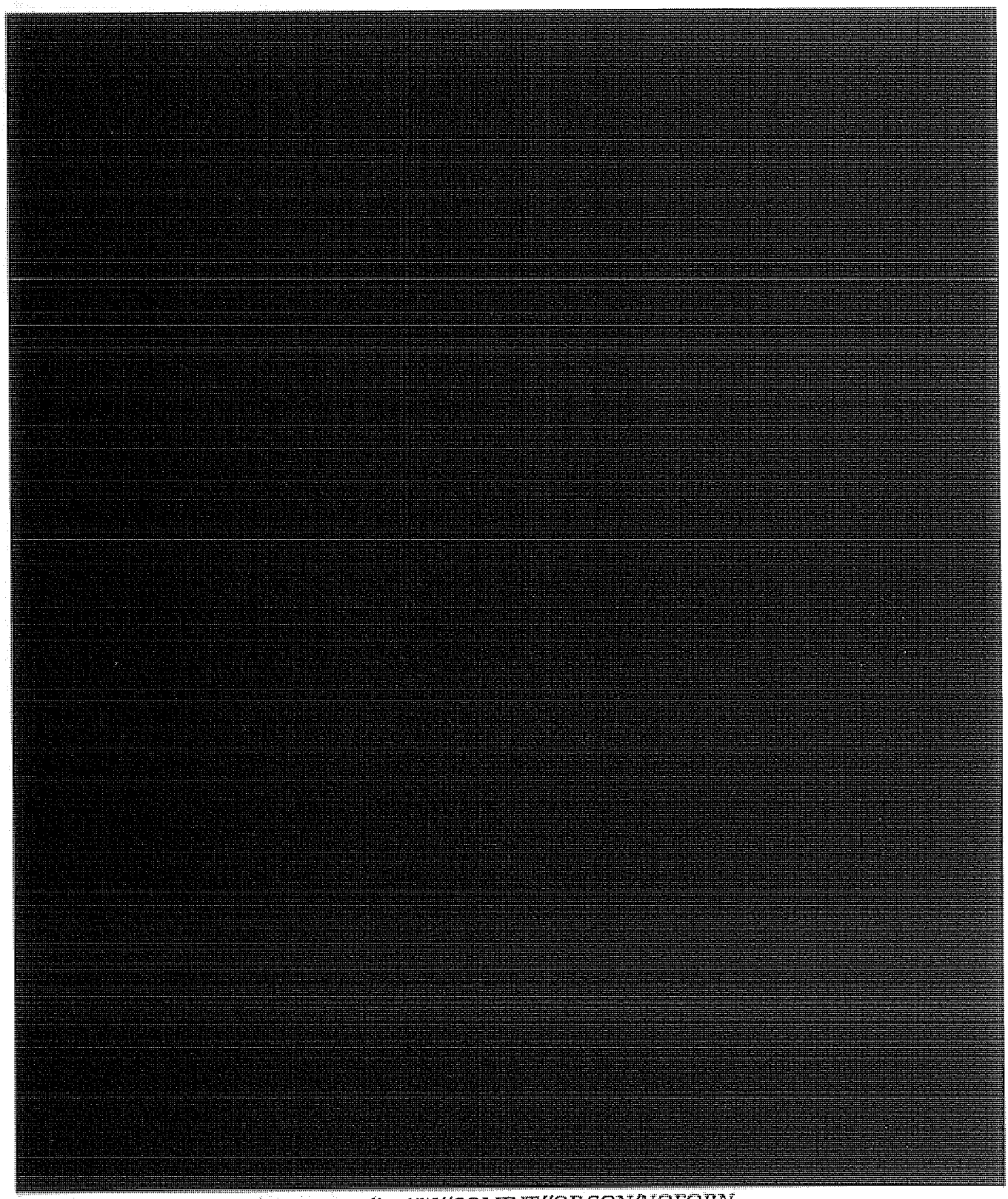
(U) PSP Information	(U) Description of SIGINT Reporting
[redacted]	

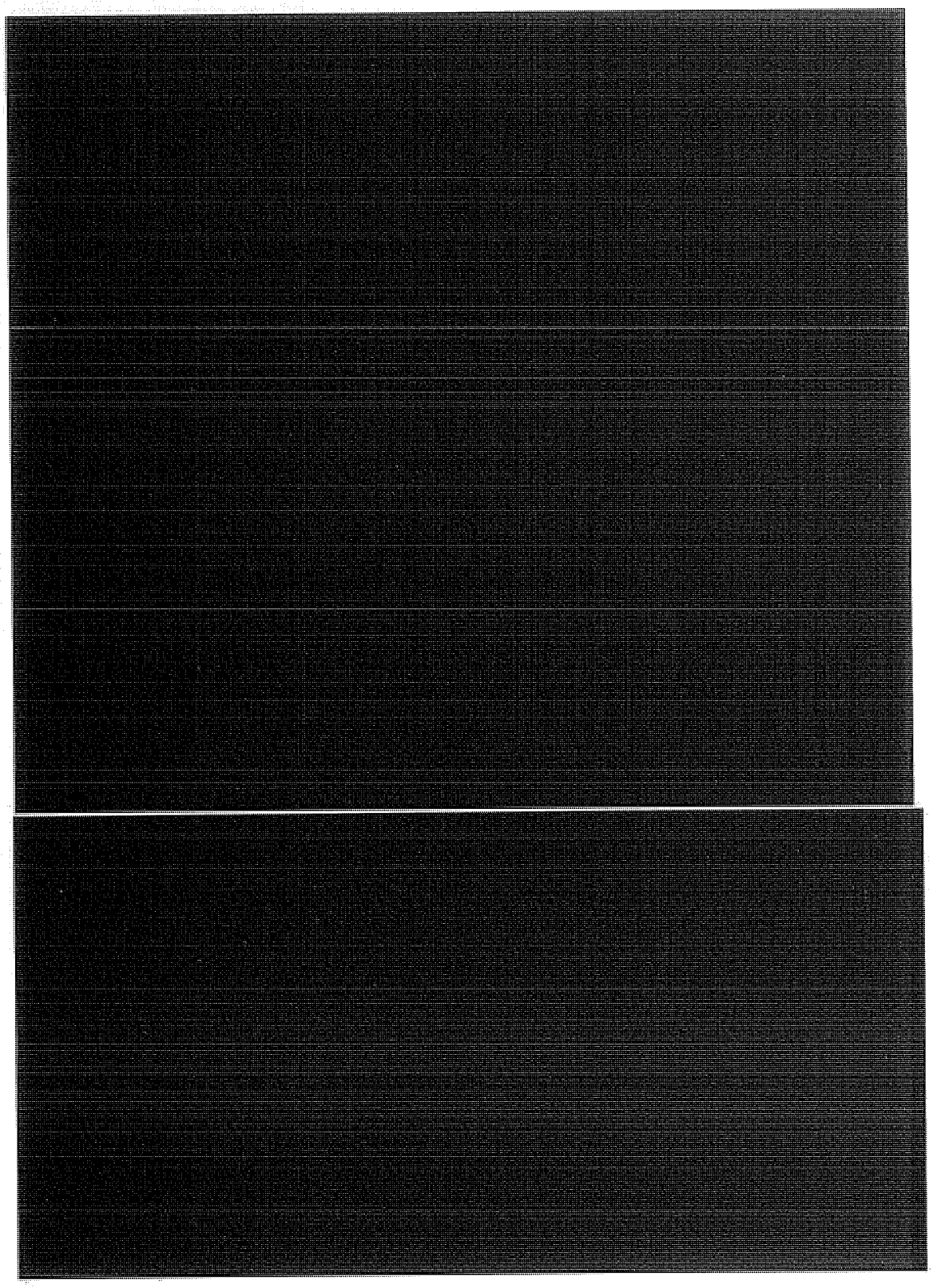
[redacted]

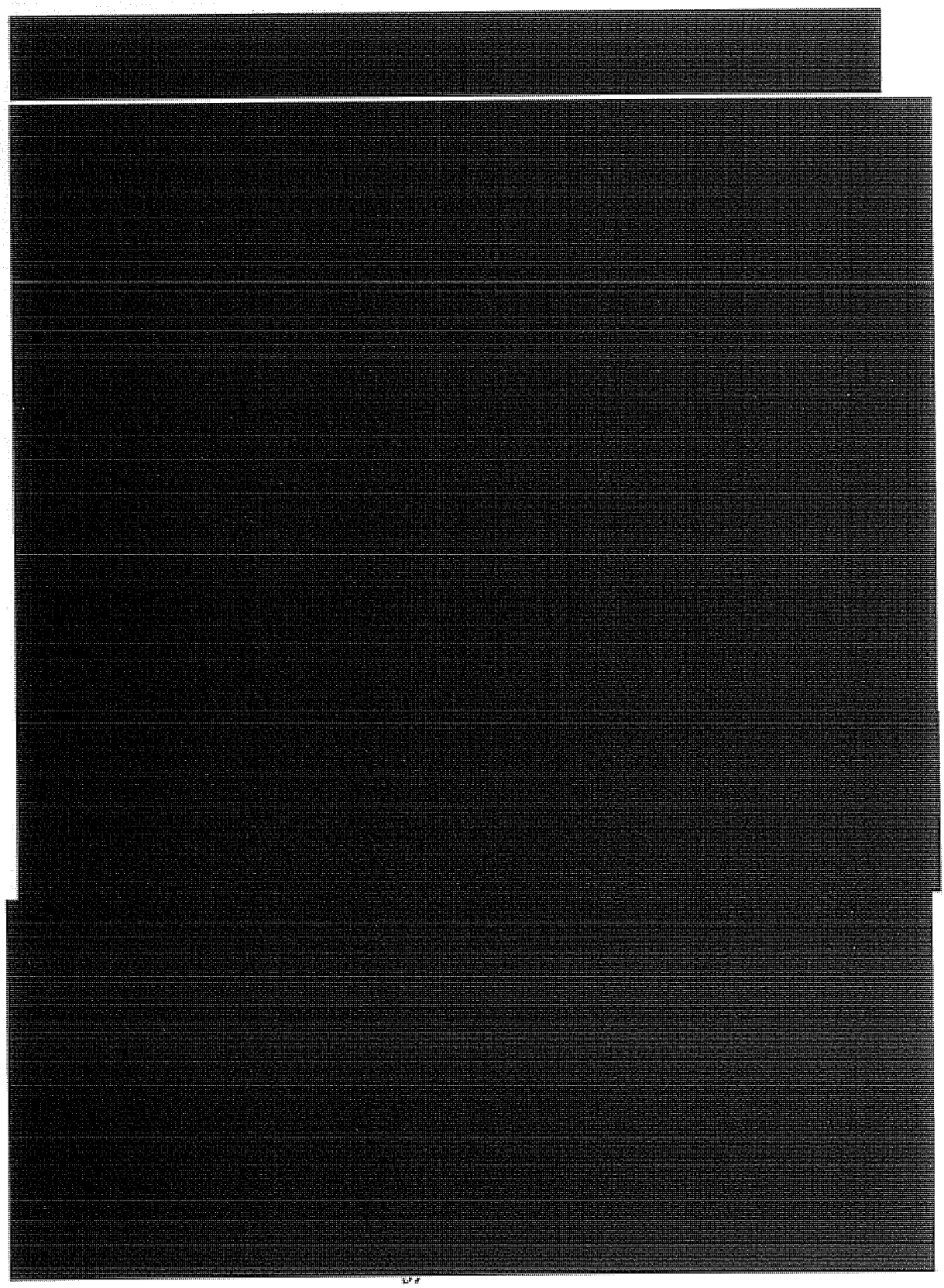




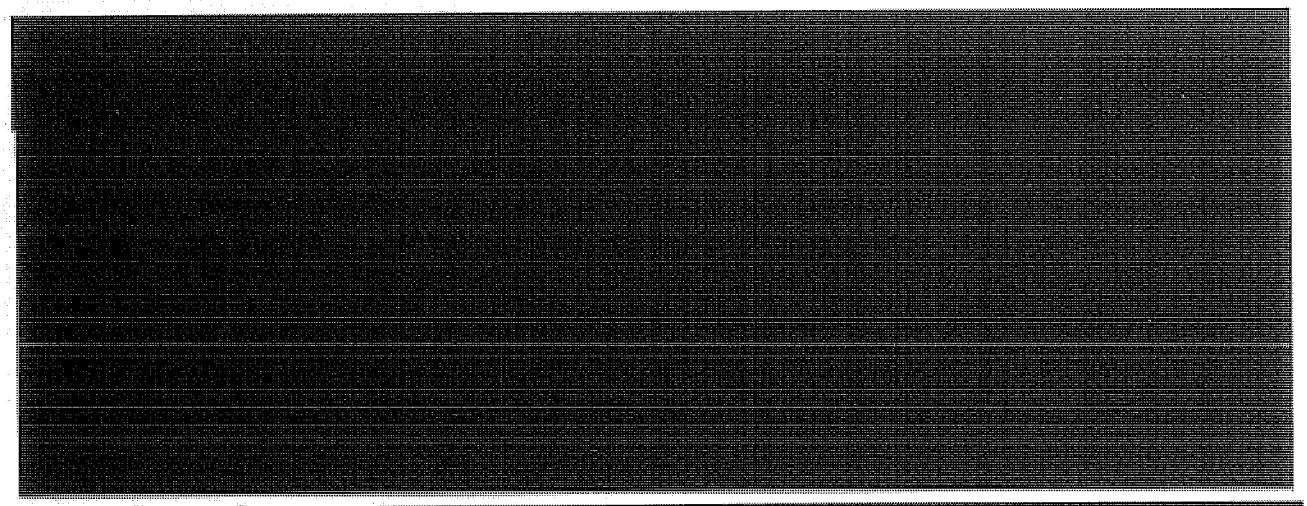


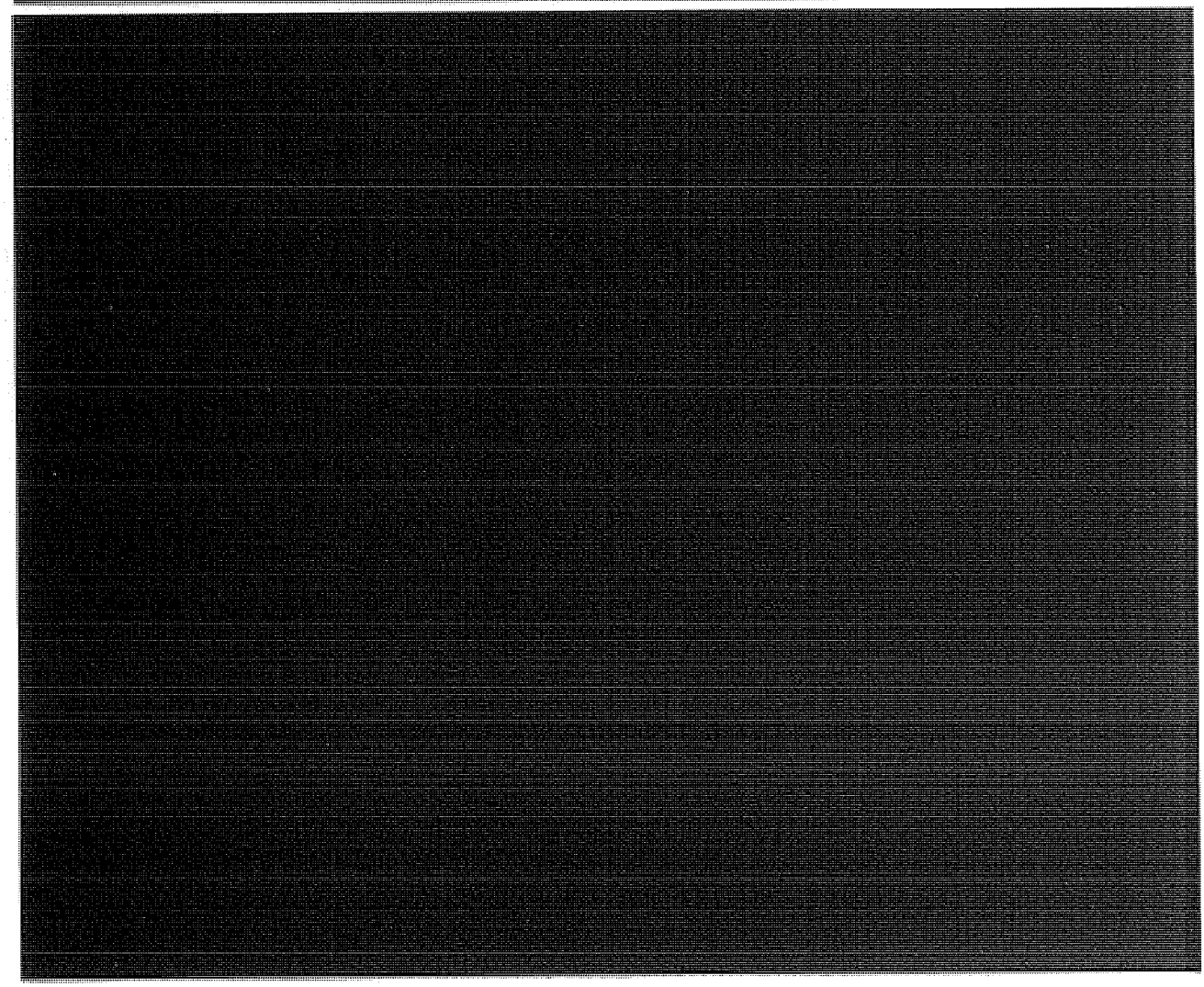


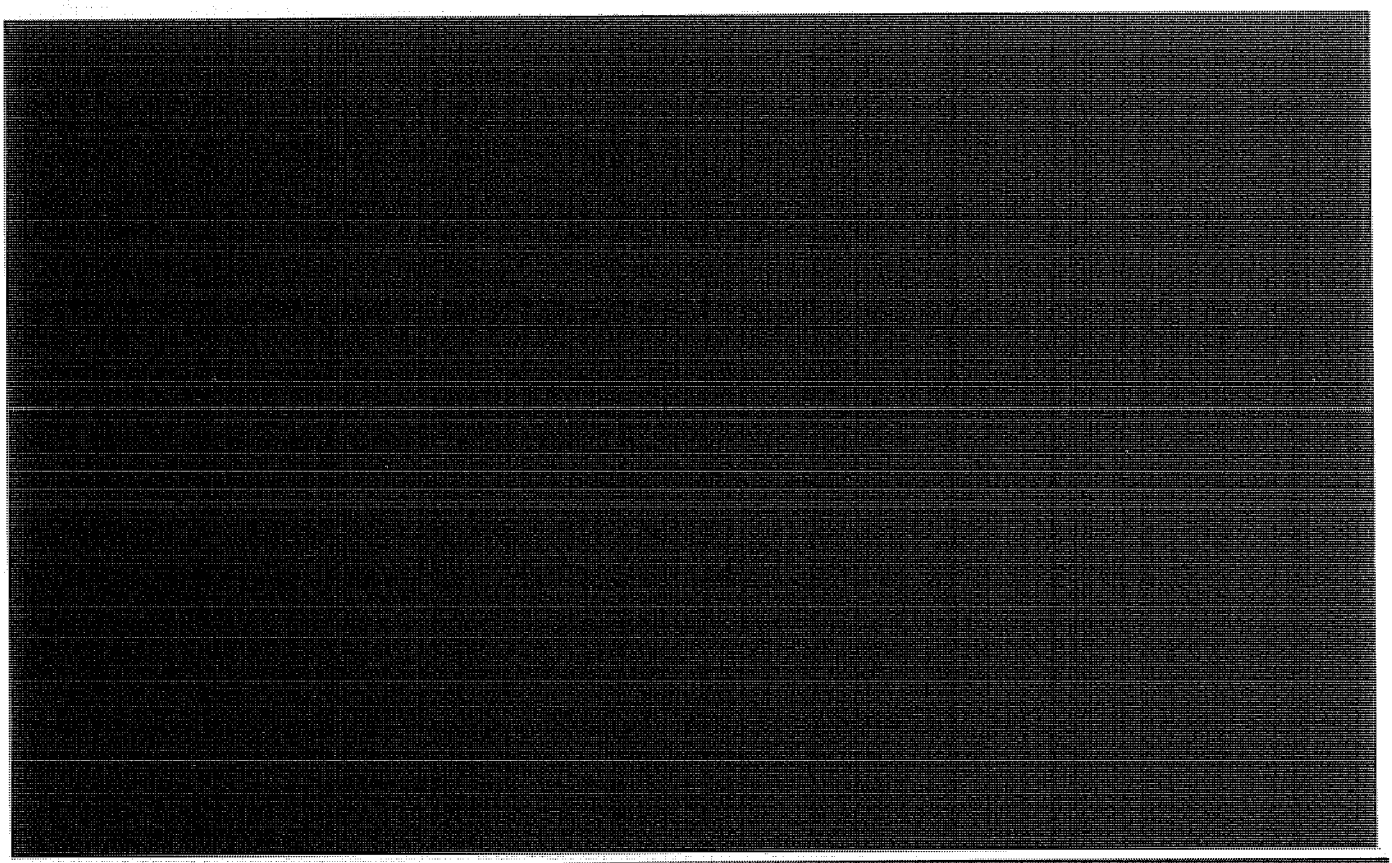


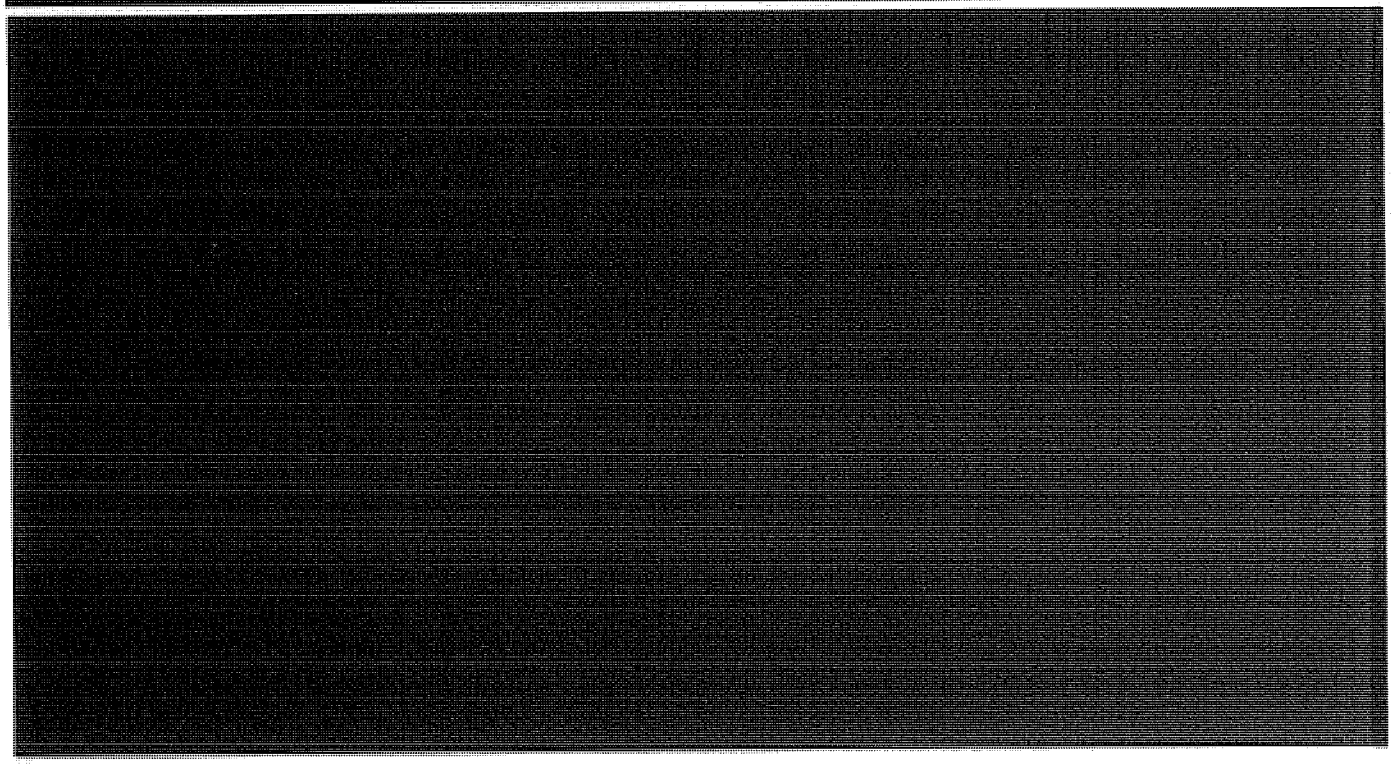


[redacted]

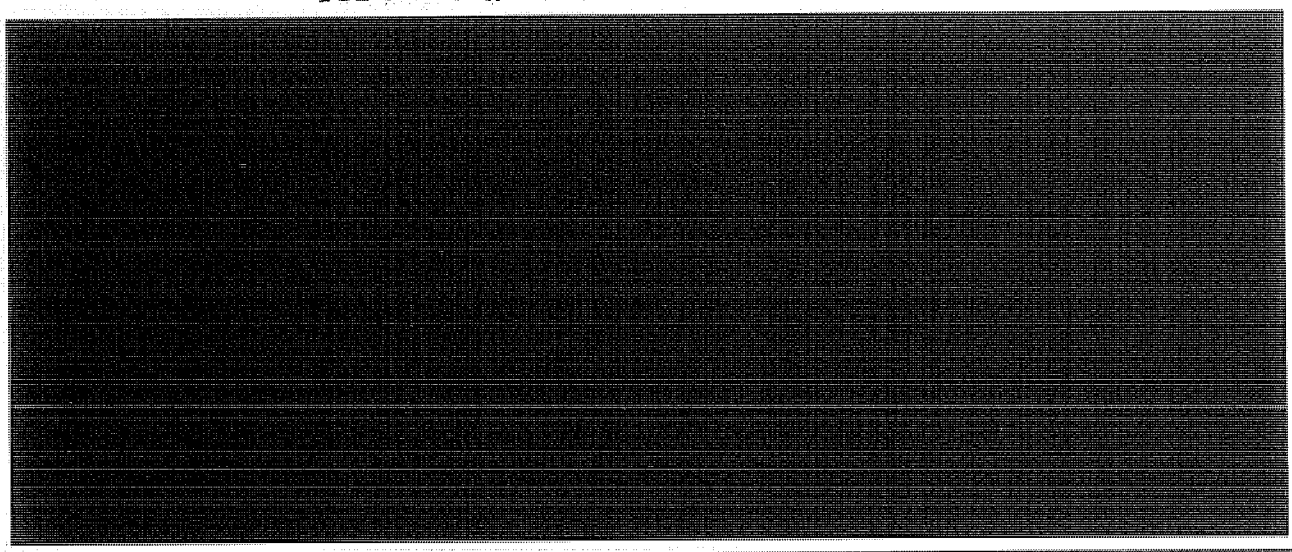




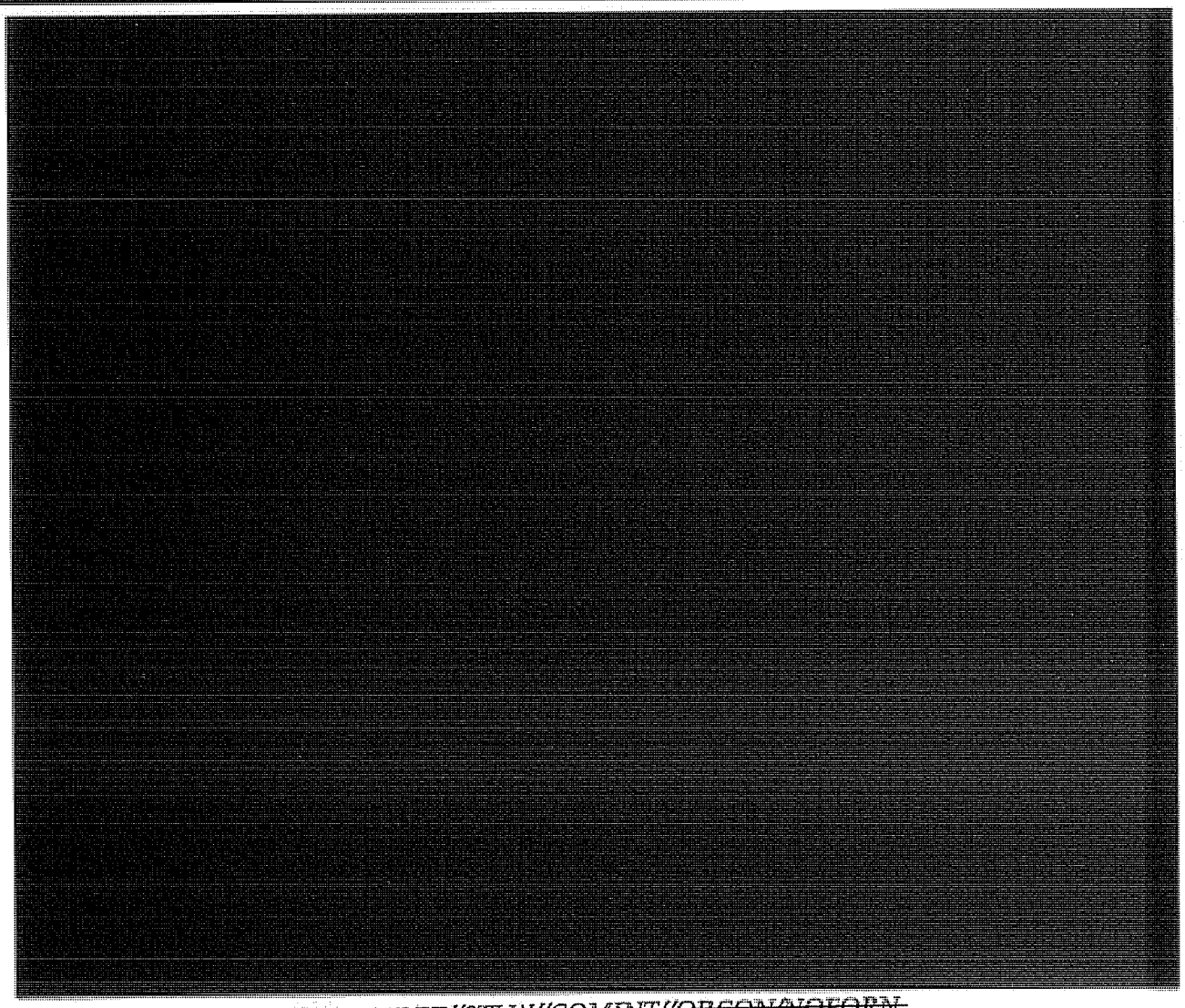


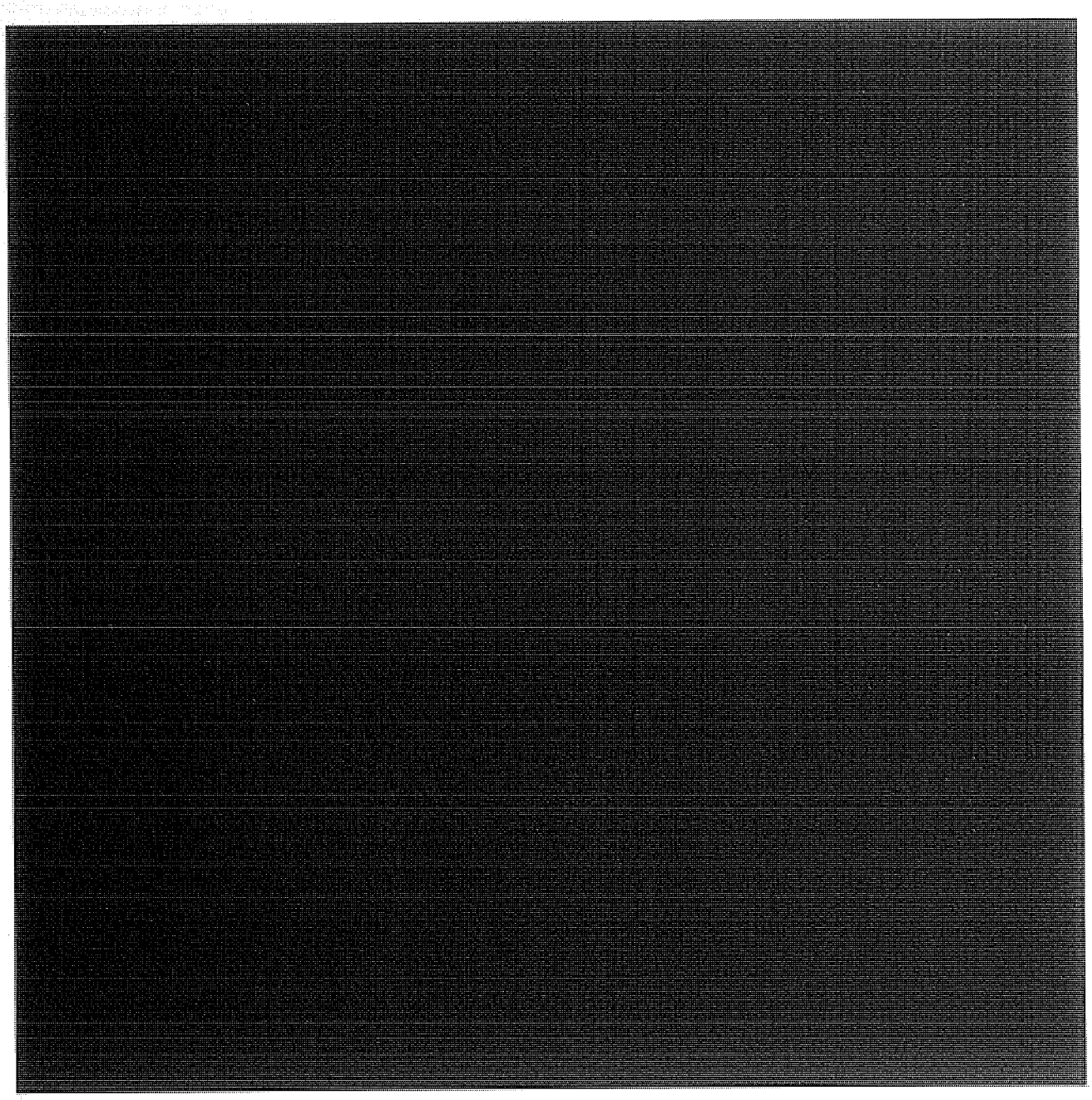


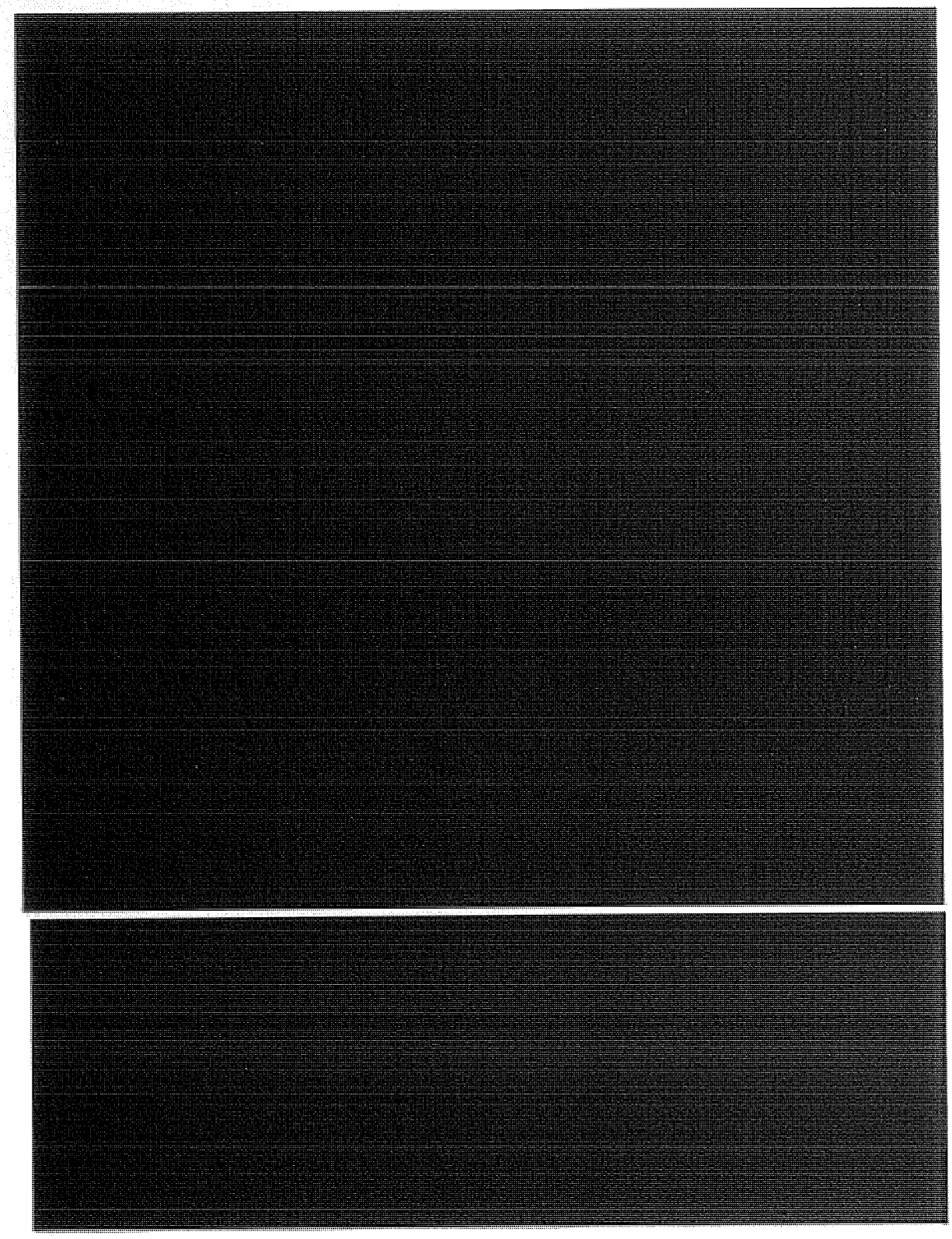
b1, b3, b7E

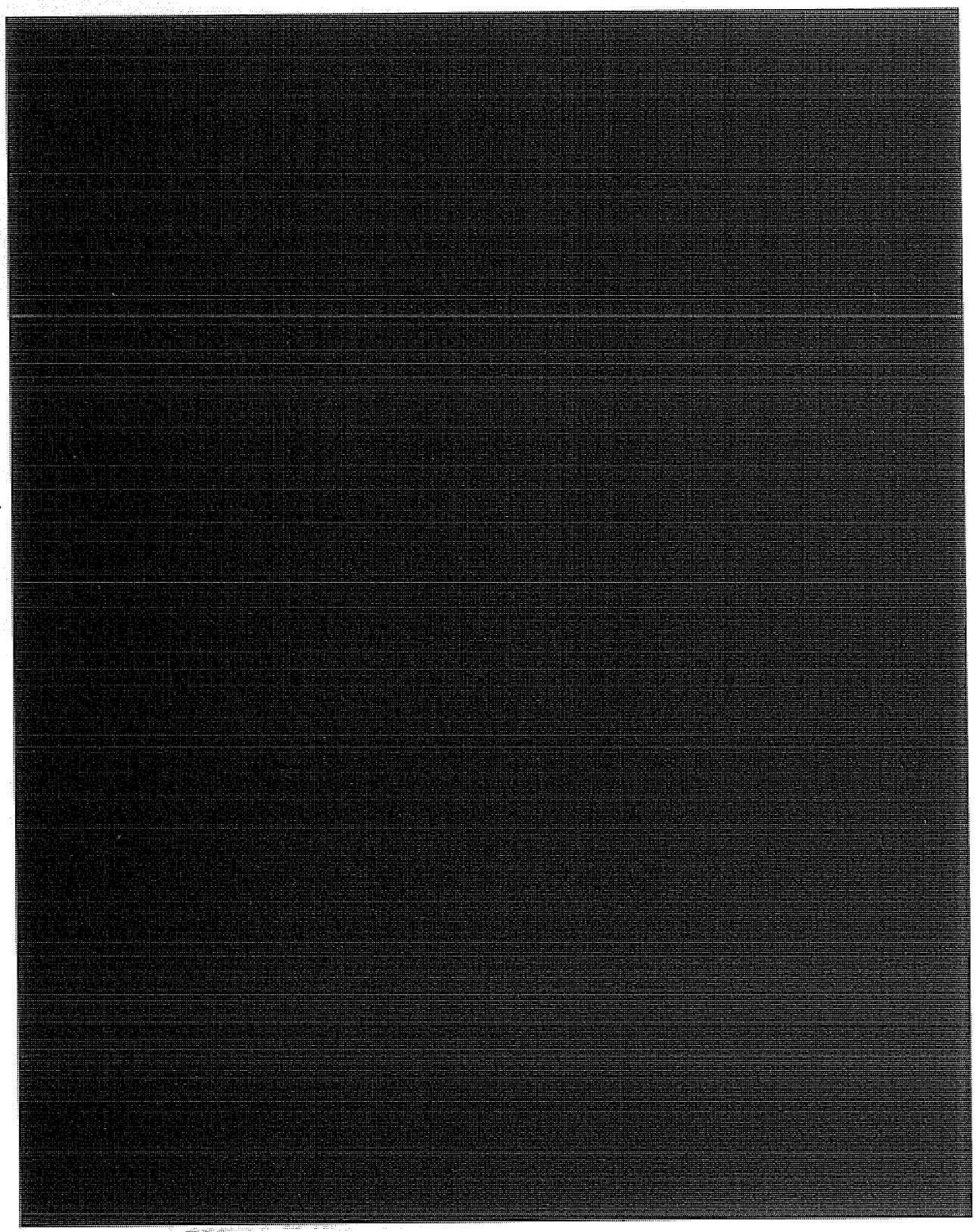


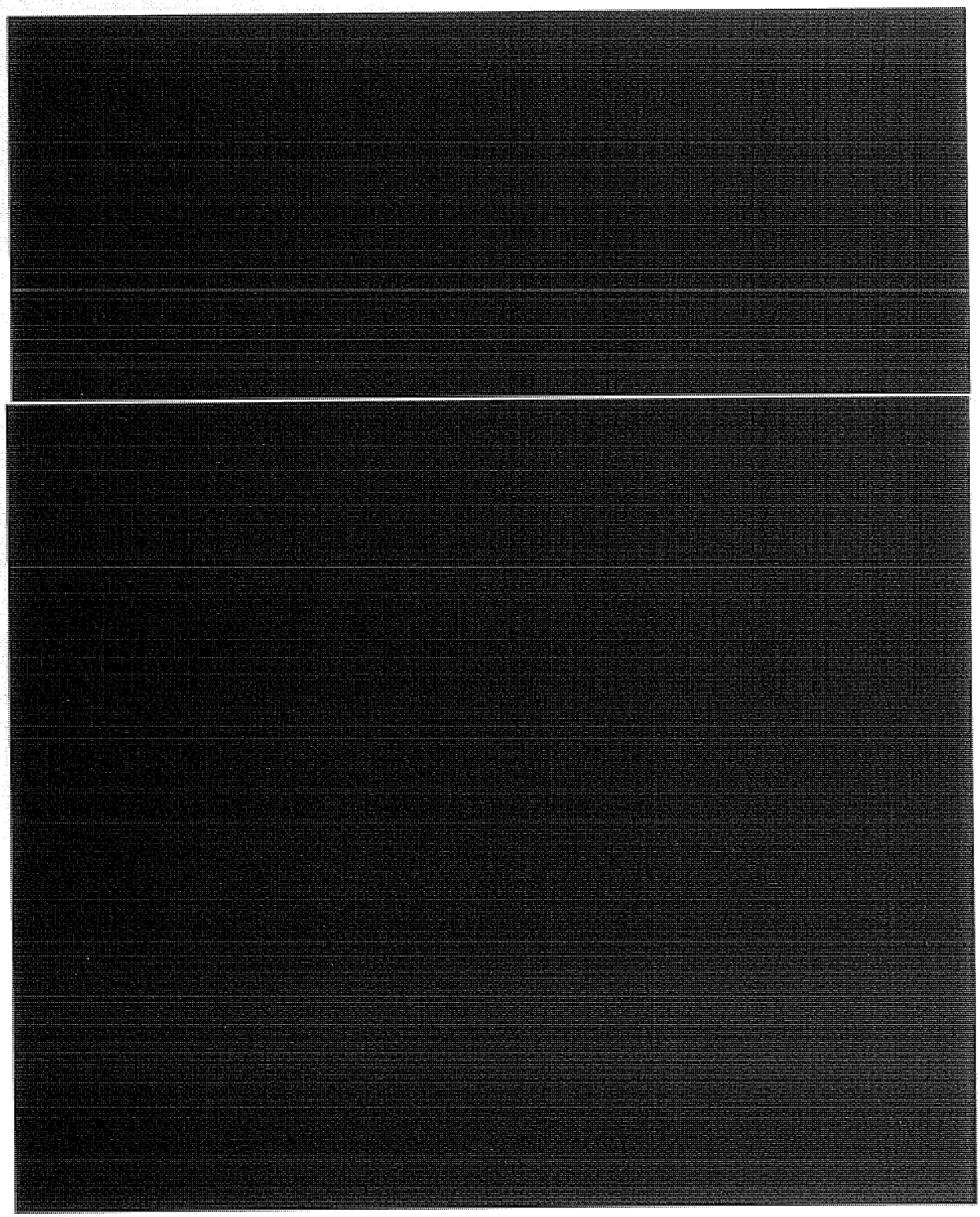
b1,
b3,
b7E

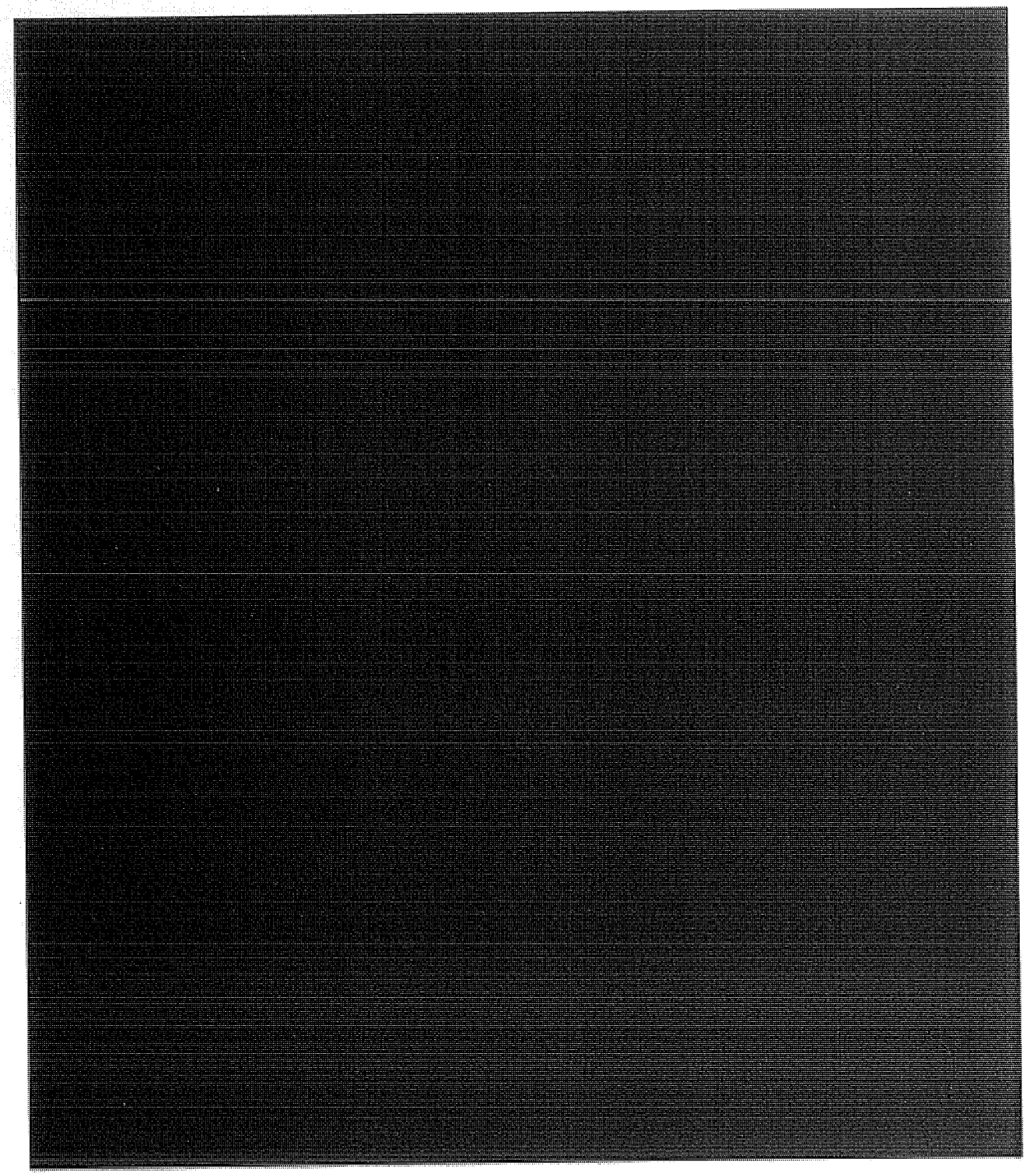












(b)(3)

(b)(3)

(b)(3)

(b) (5), (b)(3)

(b)(3), (b) (5), (b)(1)

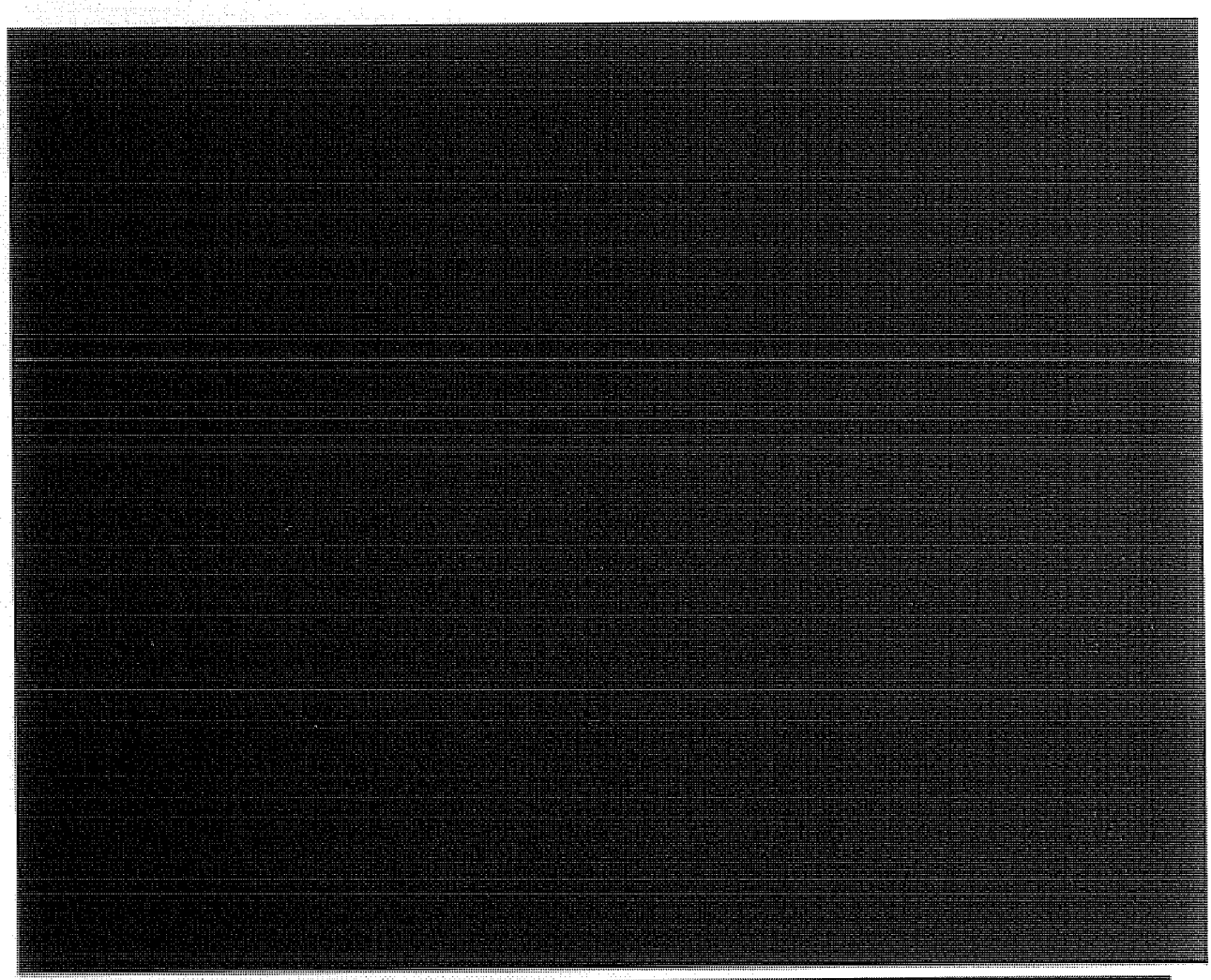
(b)(1), (b)(3)

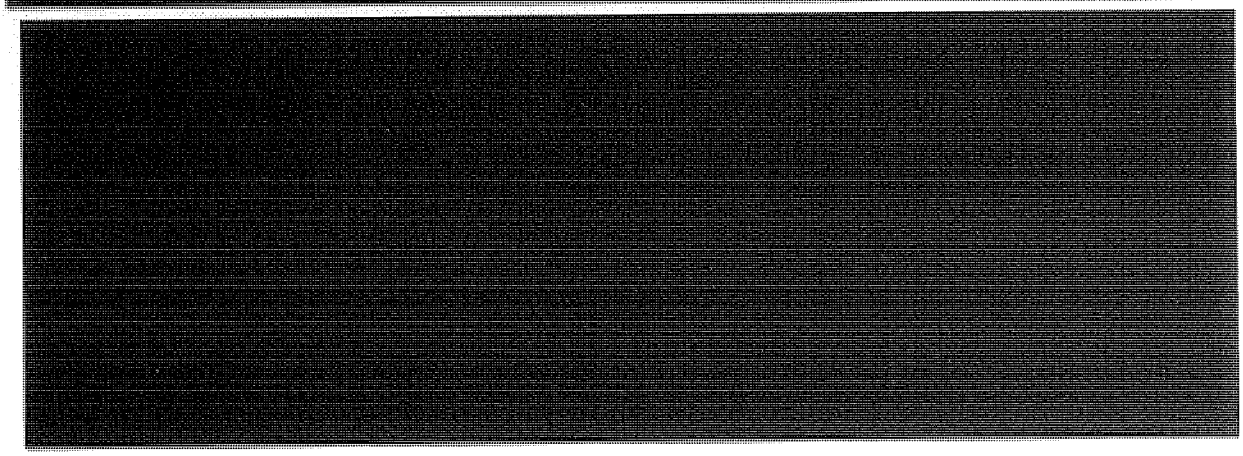
~~(TS//SI//NF)~~ On 12 March, the President directed DoJ to continue working on the legal issues, and on 15 March OLC issued a three page memorandum to the Deputy Attorney General stating that, while it had only begun to analyze the issues and was not yet prepared to issue a final opinion, it believed that (b)(1), (b)(3) types of collection authorized under the PSP were legally supportable. OLC had not yet developed a supportable argument to justify

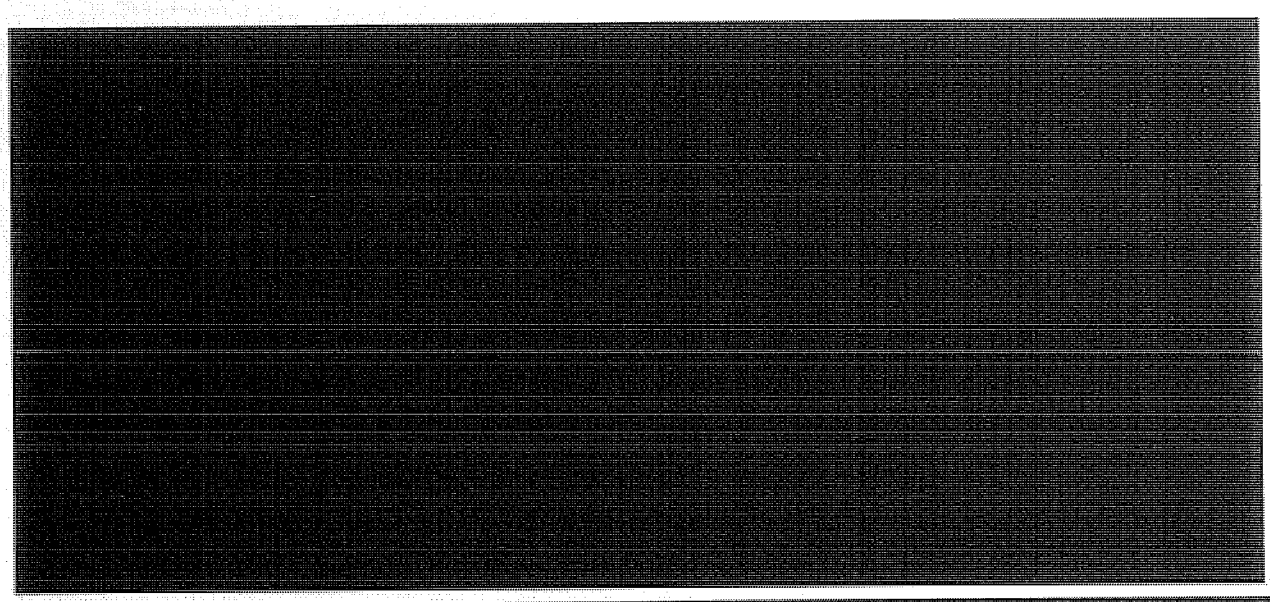
(b)(1), (b)(3), (b) (5)

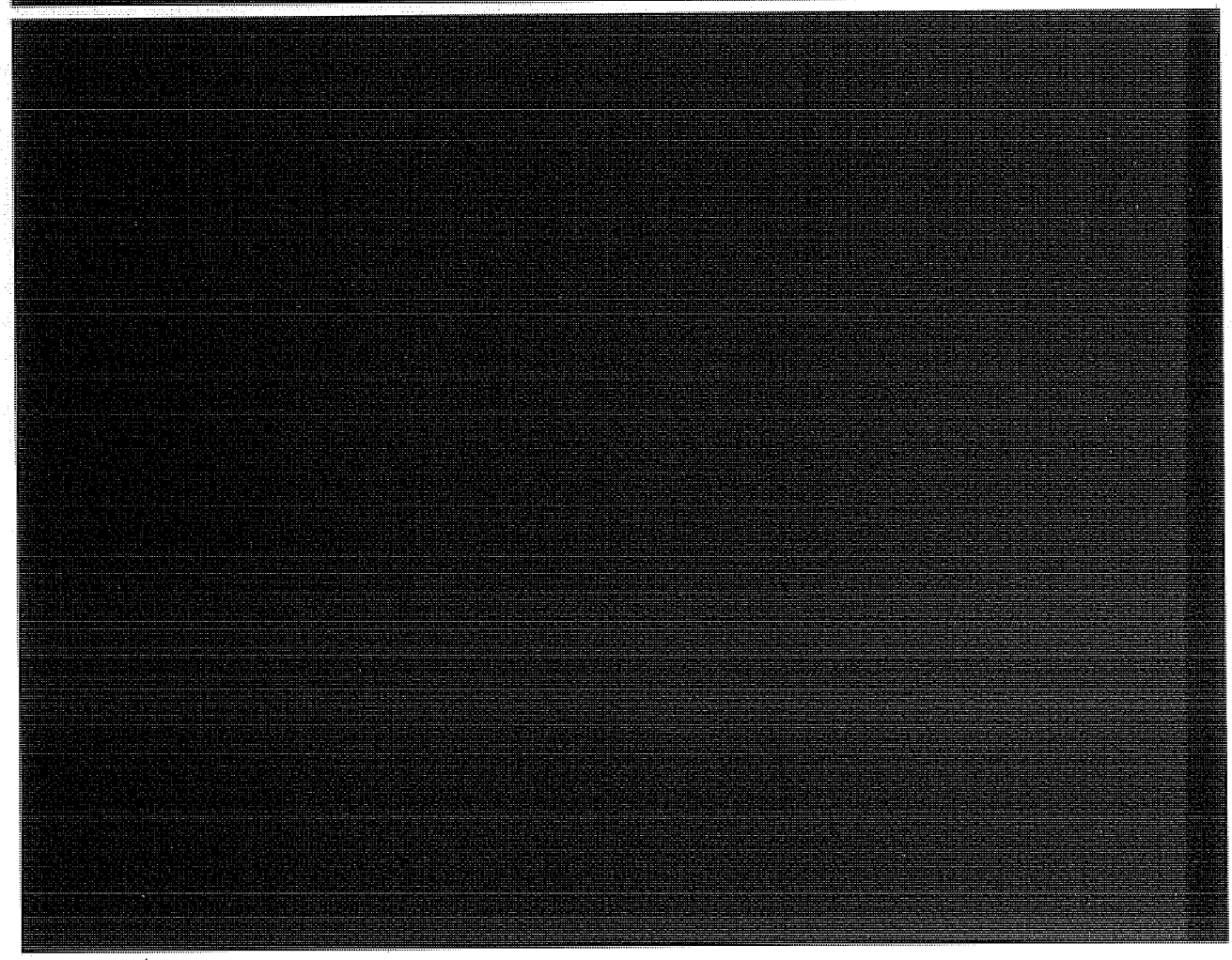
(b)(1), (b)(3)

[25] ~~(TS//SI//NF)~~ The Assistant Attorney General for OLC issued a memorandum on 6 May 2004 concluding that operation of the PSP as described in the opinion was lawful. A 16 July memorandum upheld the 6 May opinion. (b) (5)



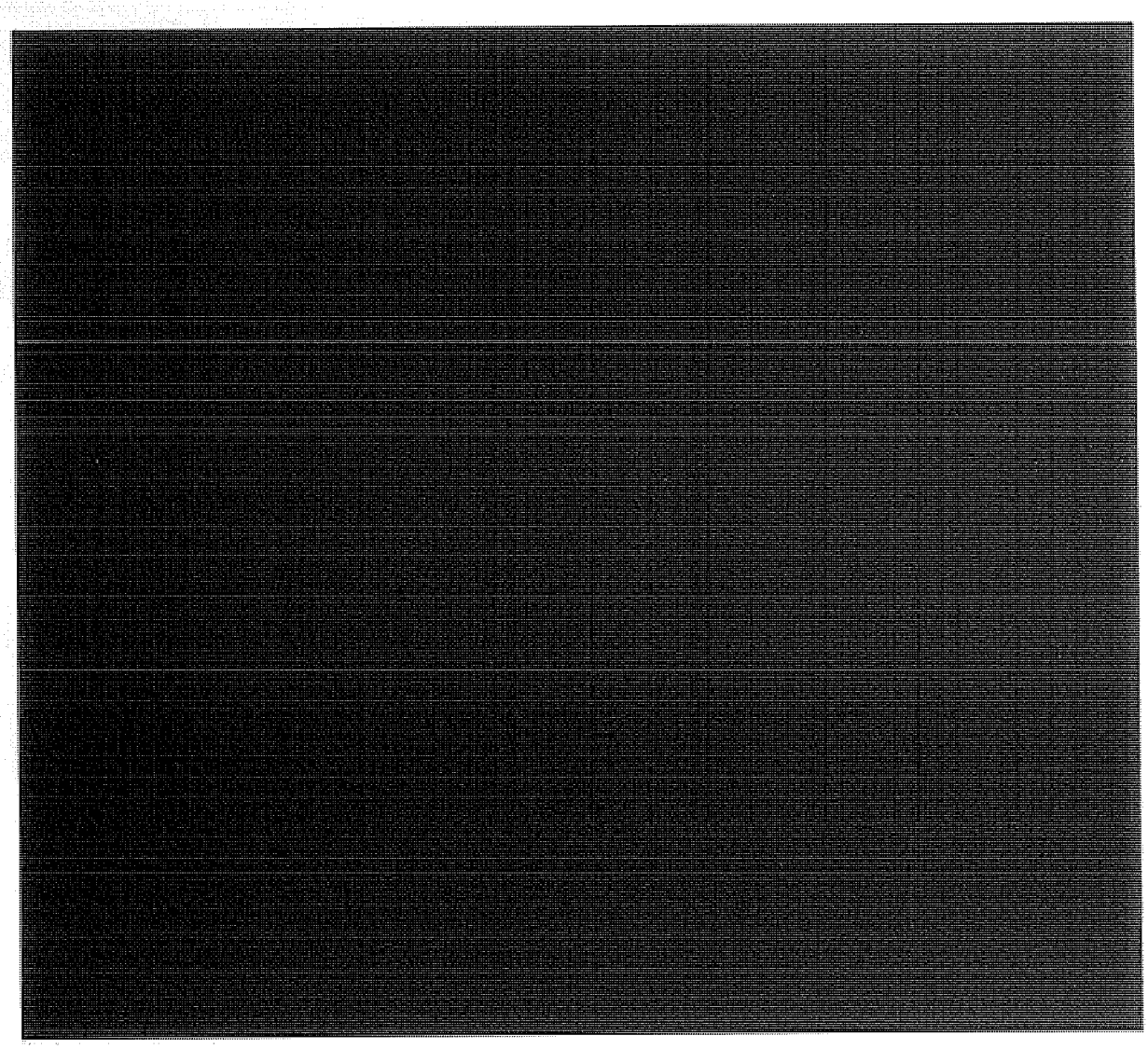




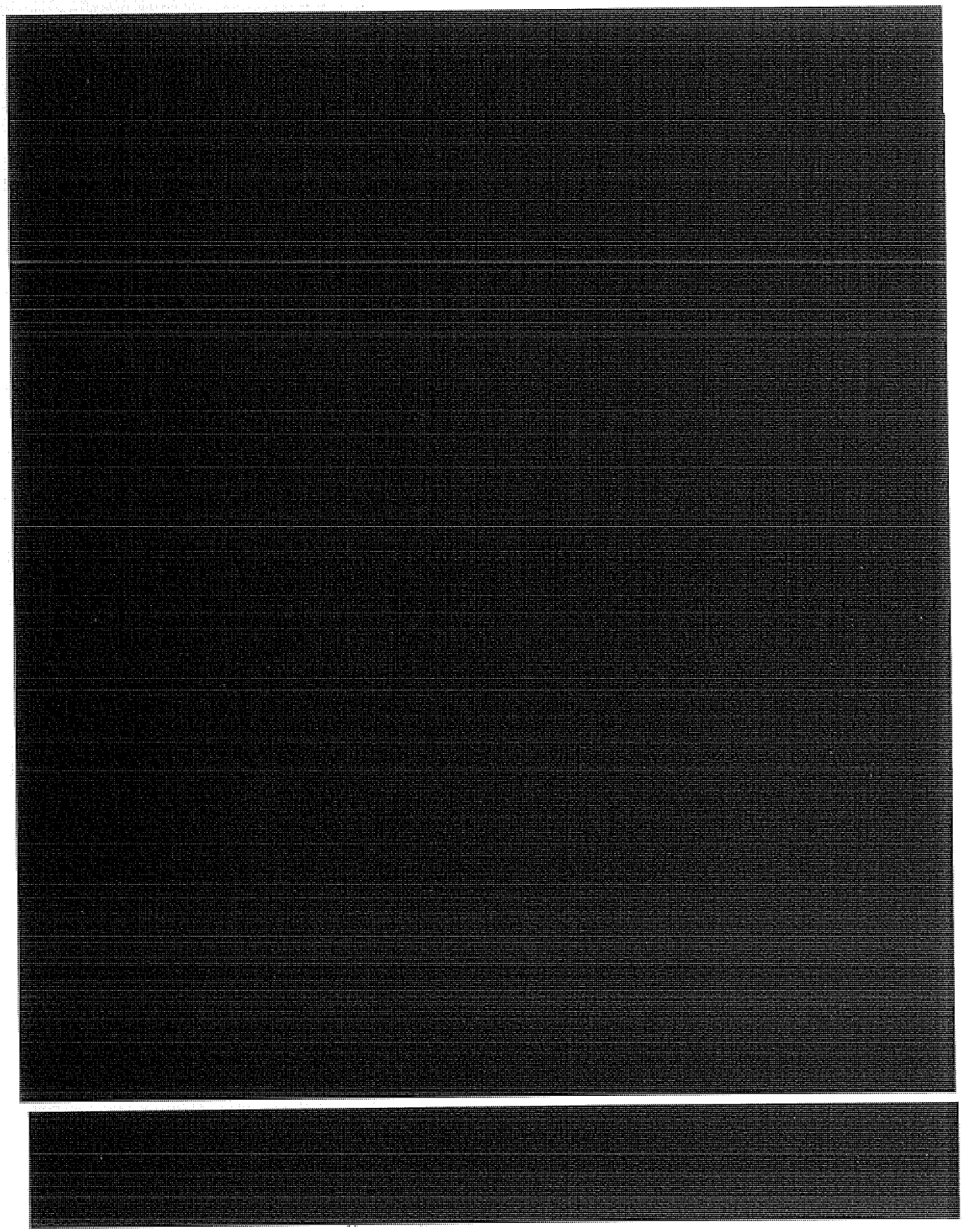


[redacted]

[27] ~~(TS//SI//NF)~~ The minimization probable cause standard states that the Agency may target for collection, communications for which there is probable cause to believe that one of the communicants is a member or agent of [redacted] and the communication is to or from a foreign country.



This page intentionally left blank.



[redacted]

(U//~~FOUO~~) The OIG issued a report for each of the 13 investigations and reviews described above. Ten reports on PSP activity resulted in 11 recommendations to management; 10 have been closed, and one remains open. Three reports on FISC-approved activity previously authorized by the PSP contained nine recommendations to management; three have been closed and six remain open.

~~(TS//STLW//SI//OC/NF)~~ Beginning in January 2007, violations that had occurred under the Authorization and violations related to PSP activity transitioned to court orders were reported quarterly to the President's Intelligence Oversight Board (through the Assistant to the Secretary of Defense for Intelligence Oversight).

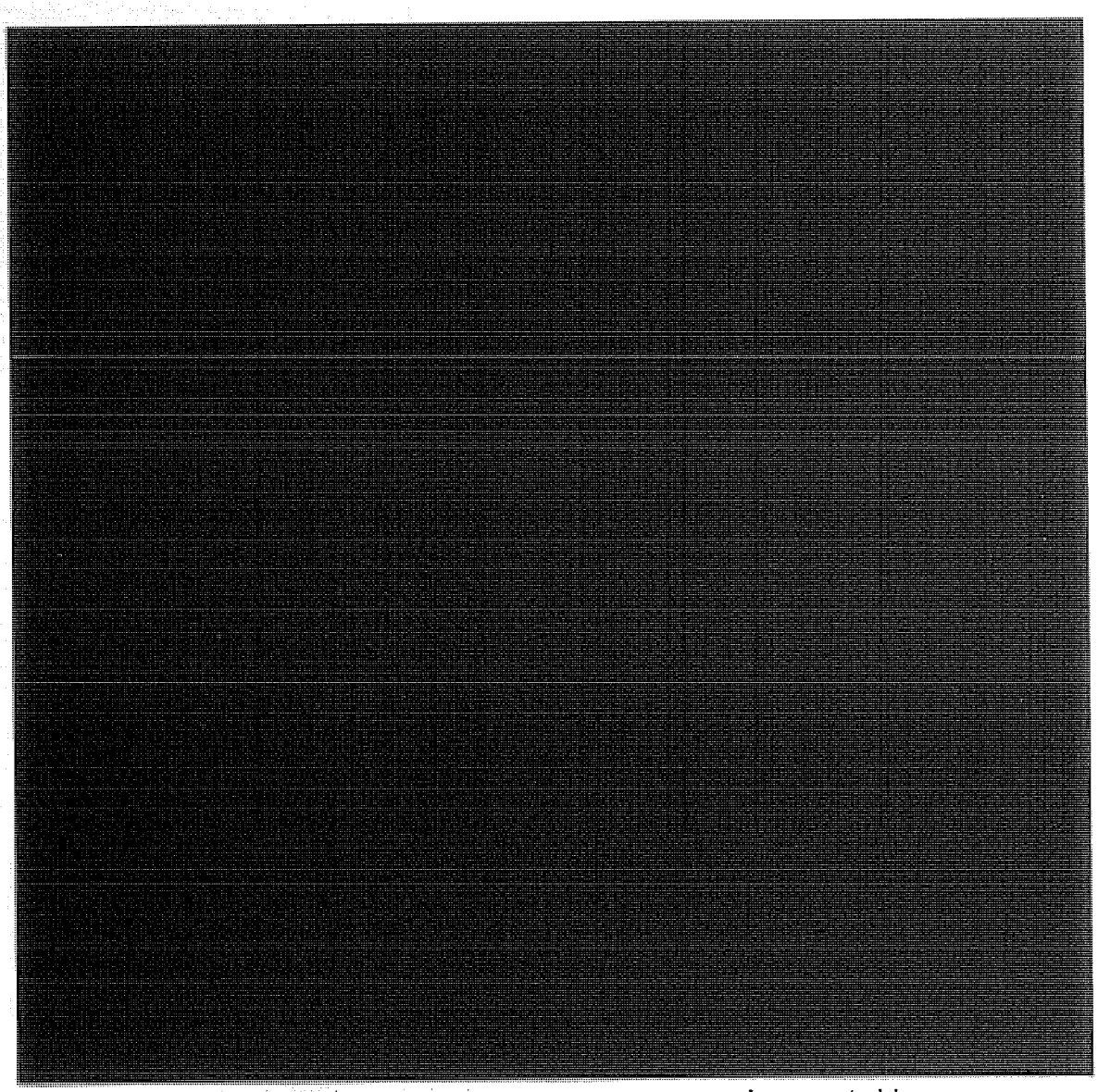
[redacted]

(U) Recently Reported Incidents

~~(TS//STLW//SI//OC/NF)~~ NSA OIG learned in late 2008 that, from approximately [redacted] collection of [redacted] All related records were purged from NSA databases in 2004; therefore, it was not possible to determine the exact nature and extent of that collection. The NSA OIG will close out this incident in an upcoming report to the President's Intelligence Oversight Board.

~~(TS//SI//NF)~~ On 15 January 2009, the Department of Justice reported to the FISC that NSA had been using an "alert list" to compare incoming business records FISA metadata against telephone numbers associated with counterterrorism targets tasked by NSA for SIGINT collection. NSA had reported to the Court that the alert list consisted of numbers for which NSA had determined that a reasonable articulable suspicion existed that the numbers were related to a terrorist organization associated [redacted] However, the majority of selectors on the alert list had not been subjected to a reasonable articulable suspicion determination. The NSA OIG has reported this incident to the President's Intelligence Oversight Board and has filed updates as required. The alert list and a detailed NSA 60-day review of processes related to the Business Records FISC order were the subject of several recent submissions to the FISC and of NSA briefings to Congressional oversight committees.

[redacted]



(U//~~FOUO~~) Other IG Program concerns were documented in the 2003-2008 reports. Presidential Notifications are listed and described in Appendix F. The 2008 report described the adequacy of Program decompartmentation plans.

(U) ACRONYMS AND ABBREVIATIONS

~~(TS//SI//NF)~~

Bps	Bits per Second
BR	Business Records
CDR	Call Detail Records
[redacted]	
CIA	Central Intelligence Agency
COMINT	Communications Intelligence
CT	Counterterrorism
DCI	Director of Central Intelligence
DNI	Director of National Intelligence
DoD	Department of Defense
DoJ	Department of Justice
EO	Executive Order
FAA	FISA Amendments Act
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
GC	General Counsel
Gbps	Gigabits per Second
HPSCI	House Permanent Select Committee on Intelligence
IG	Inspector General
LAN	Local Area Network
[redacted]	[redacted]
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
O&C	Oversight and Compliance
ODNI	Office of the Director of National Intelligence
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OIPR	Office of Intelligence Policy and Review (now the Office of Intelligence, National Security Division)
OLC	Office of Legal Counsel

PM	Program Manager
PR/TT	Pen Register/Trap & Trace
PSP	President's Surveillance Program
RFI	Request for Information
SID	Signals Intelligence Directorate
SIGINT	Signals Intelligence
SSCI	Senate Select Committee on Intelligence
[redacted]	
TS/SCI	Top Secret/Sensitive Compartmented Information

~~(TS//SI//NF)~~

(U) GLOSSARY OF TERMS

(U) COMINT	(U) Communications Intelligence – technical and intelligence information derived from foreign communications by someone other than the intended recipients
(U) E.O. 12333	(U) Executive Order 12333 - *United States Intelligence Activities* - provides goals, duties, and responsibilities with respect to the national intelligence effort. It mandates that certain activities of U.S. intelligence components are to be governed by procedures issued by agency heads and approved by the Attorney General.
(U) FISA	(U) The Foreign Intelligence Surveillance Act of 1978, as amended, governs the conduct of certain electronic surveillance activities within the United States to collect foreign intelligence information.
(U) [redacted]	~~(S//SI//NF)~~ Analytic tool for contact chaining used by analysts to do target discovery by quickly and easily navigating global communications metadata
~~(TS//SI//NF)~~ METADATA	~~(TS//SI//NF)~~ Header, router, and addressing-type information, including telecommunications dialing-type data, but not the contents of the communication
(U) [redacted]	[redacted]
(U) [redacted]	~~(S//NF)~~ NSA's primary storage, search, and retrieval mechanism for SIGINT text
(U) SANITIZATION	(U) The process of disguising COMINT to protect sensitive intelligence sources, methods, capabilities, and analytical procedures in order to disseminate the information outside COMINT channels.

(U) SIGNALS INTELLIGENCE	(U) A category of intelligence comprising individually or in combination all communications intelligence (COMINT), electronic intelligence (ELINT) and foreign instrumentation intelligence (FISINT), however transmitted.
(U) TEAR LINE REPORTS	(U) Reports used to disseminate SIGINT-derived information and sanitized information in the same record. The sanitized tear line conveys the same facts as the COMINT-controlled information, while hiding COMINT as the source.
(U) TELEPHONY	(U) The technology associated with the electronic transmission of voice, fax, and other information between parties using systems historically associated with the telephone
(U) TIPPERS	[redacted]

APPENDIX A

(U) About the Review

This page intentionally left blank.

(U) About the Review

(U) Objectives

(U) The Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, which was signed into law on 10 July 2008, requires that the Inspectors General of Intelligence Community elements that participated in the President's Surveillance Program (PSP) conduct a comprehensive review of the Program. The NSA Office of the Inspector General (OIG) reviewed NSA's participation in the PSP. The specific review objectives were to examine:

- (U) The establishment and evolution of the PSP as it affected NSA
- (U) NSA implementation of the PSP, including preparation and dissemination of product under the PSP
- (U) NSA access to legal reviews of the PSP and access to information about the Program
- (U) NSA communications with and representations made to private sector entities and private sector participation
- (U) NSA interaction with the Foreign Intelligence Surveillance Court (FISC) and transition of PSP-authorized collection to court orders
- (U) Oversight of PSP activities at NSA.

(U) Scope and Methodology

(U) This review was conducted in accordance with generally accepted government auditing standards, as set forth by the Comptroller General of the United States and implemented by the audit manuals of the DoD and NSA/CSS Inspectors General.

(U) The review was conducted from 10 July 2008 to 15 May 2009 in coordination with the Inspectors General of the Department of Defense, Office of the Director of National Intelligence, CIA, and DoJ.

(U//~~FOUO~~) The scope of this review was limited to NSA's participation in the PSP from 4 October 2001 to 17 January 2007. The review included NSA activities before and after the terrorist attacks of 11 September 2001 that led to the Presidential Authorization on 4 October 2001. It also included the transition of PSP-authorized activity to FISC orders.

(~~TS//NF~~) To satisfy review objectives, we interviewed [redacted] current and former NSA personnel who participated in the PSP including NSA Directors and Deputy Director, General Counsels, Deputy General Counsels, Associate General Counsels for Operations, and the Inspector General responsible for Program oversight from August 2002 until August 2006. We also interviewed former [redacted] as well as leadership [redacted] within the Signals Intelligence Directorate.

(~~TS//SI//NF~~) Interviews of the former Director of NSA, General Hayden, the former NSA Associate General Counsel for Operations, [redacted] were conducted with other IG offices involved in the joint PSP review.

(U//~~FOUO~~) We requested White House documentation of meetings at which General Hayden or NSA employees discussed the PSP or the Terrorist Surveillance Program with the President, Vice President, or White House personnel, but did not receive a response before publication of this report.

(~~TS//SI//NF~~) [redacted]

(U//~~FOUO~~) We reviewed NSA records dated 27 July 1993 to 10 July 2008 that pertained to review objectives. Records included NSA policies and regulations, correspondence, e-mail, briefings, notes, reports, calendars, and database reports.

(~~S//NF~~) Numbers of selectors tasked and reports issued were based on information provided by the PSP Program Management Office and were not independently verified during this review.

(U//~~FOUO~~) Information about individuals cleared for access to Program information was based on records provided by the PSP Project Security Officer and were not independently verified during this review.

(U) Prior Coverage

(U//~~FOUO~~) The OIG began oversight of the PSP and related activities in August 2002 and issued twelve reports dated 21 February 2003 through 30 June 2008 (Appendix E.) The OIG also issued 14 Presidential notifications from March 2003 to October 2006 (Appendix F). Detailed discussion of the OIG's oversight of the PSP is included in Section VIII of this report.

~~(TS//SI//NF)~~ As portions of the Program were transitioned to FISC orders for the collection of internet metadata and telephony business records, the OIG reviewed the execution and adequacy of controls in ensuring compliance with the orders. The OIG did not test the efficacy of controls for metadata collected under the authority of the PSP or court orders. Three reports summarized OIG investigations into possible misuse of the Authority or violations of FISC orders. One report summarized the OIG's oversight of the PSP, and the last report reviewed the adequacy of Program decompartmentation plans.

This page intentionally left blank.

APPENDIX B

(U) The Presidential Authorizations

This page intentionally left blank.

(U) The Presidential Authorizations

~~(TS//STLW//SI//OC/NF)~~ The Authorization documents that contained the terms under which NSA executed special Presidential authority were addressed to the Secretary of Defense and were titled "*Presidential Authorization for Specified Electronic Surveillance Activities during a Limited Period to Detect and Prevent Acts of Terrorism within the United States.*" The first Authorization consisted of eight paragraphs, and all but one subsequent Authorization consisted of nine. There were 43 Authorizations, two modifications, and one document described as (b)(1), (b)(3)

Description of Authorization contents by paragraph:

(U) Paragraph 1 - The President's Conclusions

~~(TS//STLW//SI//OC/NF)~~ The first paragraph referred to the 11 September 2001 terrorist attacks and the President's directions [to the Secretary of Defense] on employing U.S. Armed Forces. The first Authorization contained statements on the President's conclusions based on information about terrorist capabilities; this statement became the second paragraph in subsequent Authorizations. After the first Authorization, paragraph one included references to all previous versions of the Authorization and the dates they were signed by the President.

(U) Paragraph 2 - Terrorism Threat

~~(TS//STLW//SI//OC/NF)~~ After the first Authorization, the second paragraph stated that the President based his conclusions about terrorist capabilities on information provided by the DCI, including an attached terrorism threat assessment, a document that consisted of five or more pages and was signed by the DCI (later by the DNI) and the Secretary of Defense.

(U) Paragraph 3 - Considerations

~~(TS//STLW//SI//OC/NF)~~ The third paragraph contained the President's considerations in authorizing electronic surveillance, including the potential for deaths, injuries, and destruction from acts of terrorism, their probability, the need for action and secrecy, and intrusion into privacy, its reasonableness, and alternatives. In the first Authorization the considerations were in paragraph two.

~~(TS//STLW//SI//OC/NF)~~ Paragraph three of the first Authorization stated the President's determination that an

"extraordinary emergency" existed made electronic surveillance without a court order a compelling Government interest.[1]

~~(TS//STLW//SI//OC/NF)~~ Paragraph 4 - Authorized Electronic Surveillance

~~(TS//STLW//SI//OC/NF)~~ Paragraph four contains the President's statement of the basis for issuing the authority and the substantive description of the electronic surveillance that he authorized and directed. The President states that he is acting pursuant to Article II of the Constitution, including the executive power, his authority as Commander in Chief of the Armed Forces, his duty to preserve, protect and defend the Constitution, and the Authorization for Use of Military Force Joint Resolution (Public Law 107-40), with due regard for the Fourth Amendment. There were major and minor changes in that description, resulting in seven versions of paragraph four over approximately six years.

~~(TS//SI//NF)~~ Changes to Authorization Language on Electronic Surveillance

~~(TS//STLW//SI//OC/NF)~~

Version/Date	Description of Changes to Authorization Language
First Authorization 4 October 2001	Authorized NSA to acquire the content and associated metadata of telephony and Internet communications including wire and cable communications carried into or out of the United States for which there was probable cause to believe that one of the communicants was (b)(1), (b)(3) that one communicant was engaged in or preparing for acts of international terrorism.[2] This was the only version of the Authorization to use the term "probable cause." Version 1 also authorized the acquisition of telephony and Internet metadata for communications with at least one communicant outside the United States or for which no communicant was known to be a citizen of the United States. Paragraph four included the authority to

[1](U) The third paragraph was marked with the number three in two places until the error was corrected in the September 2003 authorization.
[2](U) This parenthetical condition is present in all descriptions of content collection.

Version/Date	Description of Changes to Authorization Language
	retain, process, analyze and disseminate intelligence from the communications acquired under the authority.
Version 2 2 November 2001 and 30 November 2001	Authorized NSA to acquire the content and associated metadata of communications for which there was "reasonable grounds to believe" that one of the communicants was (b)(1), (b)(3) that one communicant was outside the United States and was engaged in or preparing for acts of international terrorism.[3] This change to the wording on collecting content eliminated the possibility of interpreting the authority to permit collection with both ends in the United States. This version also authorized the acquisition of telephony and Internet metadata for communications with at least one communicant outside the United States, with no communicant known to be a citizen of the United States, or when there were reasonable grounds to believe that the communication related to international terrorism or activities in preparation for international terrorism. Version 2 was used in two Authorization documents.
Version 3 9 January 2002 to 14 January 2004	Eliminated (b)(1), (b)(3) but was otherwise identical to the previous version. This version of the authorizing provision was used in 19 of the documents.
Version 4 11 March 2004	Stated that the Department of Defense may obtain and retain Internet and telephony metadata (b)(1), (b)(3) on the condition that search and retrieval of that information was conducted in accordance with the Authorization. The term "acquire" was defined with respect to metadata as the act of querying stored data. (b)(1), (b)(3) The provision contained the President's statement that both

[3](U) Qualified as "based on the factual and practical considerations of everyday life on which reasonable persons act."

Version/Date	Description of Changes to Authorization Language
	these clarifications were consistent with all previous Authorizations and thus approval for acting under that definition was retroactive.
Version 5 19 March 2004	Became effective in the middle of a previously authorized period as the result of a modification. NSA's authority to collect content and associated metadata was changed to specify that the terrorist groups for which there was authority to collect were al-Qa'ida, groups affiliated with al-Qa'ida, or another group that the President determined was in armed conflict with the United States. NSA's authority to [redacted] (b)(1), (b)(3)
Version 6 2 April 2004 to 10 September 2005	Also became effective in the middle of a previously authorized period as the result of a modification. NSA's authority [redacted] (b)(1), (b)(3) al-Qa'ida, a group affiliated with al-Qa'ida, or of another group that the President determined was in armed conflict with the United States. Version 6 was used in 12 of the documents.
Version 7 26 October 2005 to 8 December 2006	Added the clarification that groups affiliated with al-Qa'ida [redacted] (b)(1), (b)(3) the provision was otherwise identical to that in version 6. Version 7 and was used in the final nine documents.

~~(TS//STLW//SI//OC/NF)~~

(U//~~FOUO~~) Paragraph 5 - Detect and Prevent

~~(TS//STLW//SI//OC/NF)~~ In paragraph five, the President stated that the surveillance was essential and appropriate to

detect and prevent future acts of terrorism in the United States.

(U//~~FOUO~~) Paragraph 6 - Minimization

~~(TS//STLW//SI//OC/NF)~~ Paragraph six directed that information concerning American citizens be minimized to the extent consistent with the mission and with the Authorization.

(U//~~FOUO~~) Paragraph 7 - Notifying Congress

~~(TS//STLW//SI//OC/NF)~~ Paragraph seven stated that notification of the Authorization outside the executive branch would be deferred, but the President stated his intent to notify Congress when consistent with national defense. When select members of Congress were briefed on the Program, information on the briefings was contained in paragraph eight.

(U) Paragraph 8 - Other Notifications

~~(TS//STLW//SI//OC/NF)~~ The initial Authorization specified that collection would cease 30 days after signature and required reporting on changes in circumstances underlying the Authorization. After the initial Authorization, paragraph eight contained a statement on restricting notifications to U.S. Government officials outside the executive branch or it named individuals, by title, who had been informed since the previous Authorization period expired.

(U) Paragraph 9 - Expiration

~~(TS//STLW//SI//OC/NF)~~ After the initial Authorization, the exact date of expiration was specified in paragraph nine.

(U//~~FOUO~~) Paragraph 10 - "The President's Ultimate Responsibility"

~~(TS//STLW//SI//OC/NF)~~ The Authorization signed in March of 2004 – the only one not signed by the Attorney General or a Deputy Attorney General– is also the only Authorization that contains a paragraph ten. This paragraph contained a legal argument about the President's ultimate responsibility to interpret the law on behalf of the executive branch and his authority for issuing the Authorization.

(b)(1), (b)(3)

(U//~~FOUO~~) Signature of President

~~(TS//STLW//SI//OC/NF)~~ The Authorizations were signed by the President, followed by a place and date of signature. All but one authorization was signed in Washington, D.C.

(U) Other Signatures

~~(TS//STLW//SI//OC/NF)~~ Under the phrase "approved for form and legality," the Attorney General signed all but one of the Authorizations. The other authorization and the two modifications were signed by the Counsel to the President.

(U) Handwritten Note

~~(TS//STLW//SI//OC/NF)~~ The first 2 and the last 29 Authorizations, both modifications, and (b)(1), (b)(3) have a handwritten note signed by the Secretary of Defense (or Deputy Secretary of Defense) directing the NSA or the Director of NSA to execute the document.

APPENDIX C

(U) Timeline of Key Events

This page intentionally left blank.

(U) Timeline of Key Events

(U//~~FOUO~~) This timeline includes key events that occurred during NSA's implementation of the President's Surveillance Program (PSP). In addition to issuances of the Authorization, the timeline includes selected communications between NSA and Congress, the Foreign Intelligence Surveillance Court (FISC), [redacted] Because the timeline is limited to documented events and communications, it is not all-inclusive.

~~(TS//STLW//SI//OC/NF)~~

Date	Event
2001	
4-Oct-01	**1st Presidential Authorization signed**
4-Oct-01	General Hayden briefs White House (President, Vice President [VP], VP Counsel, VP Chief of Staff, White House Counsel)
[redacted]	[redacted]
25-Oct-01	NSA briefs Chair and Ranking Member of House Permanent Select Committee on Intelligence (HPSCI), Chair and Vice Chair of Senate Select Committee on Intelligence (SSCI)
2-Nov-01	**2nd Presidential Authorization signed**
[redacted]	[redacted]
14-Nov-01	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
30-Nov-01	**3rd Presidential Authorization signed**
4-Dec-01	NSA briefs Chair, Senate Defense Appropriations Subcommittee, and Ranking Member, Senate Defense Appropriations Subcommittee
5 Dec 01	NSA briefs FBI Director Mueller
[redacted]	[redacted]
2002	
9-Jan-02	**4th Presidential Authorization signed**
[redacted]	[redacted]
11-Jan-02	NSA briefs Department of Justice, Office of Intelligence Policy and Review (DoJ, OIPR), James Baker
31-Jan-02	NSA briefs FISC Presiding Judge Lamberth
[redacted]	[redacted]
5-Mar-02	NSA briefs Chair and Ranking Member, HPSCI, and Vice Chair, SSCI
14-Mar-02	5th Presidential Authorization signed
[redacted]	[redacted]

Date	Event
10-Apr-02	NSA briefs Chair SSCI
18-Apr-02	6th Presidential Authorization signed
[redacted]	[redacted]
17-May-02	NSA briefs incumbent FISC Presiding Judge Kollar-Kotelly
22-May-02	7th Presidential Authorization signed
[redacted]	[redacted]
12-Jun-02	NSA briefs Chair, HPSCI, and Ranking Member HPSCI
24-Jun-02	8th Presidential Authorization signed
[redacted]	[redacted]
8-Jul-02	NSA briefs Chair and Ranking Member SSCI
30-Jul-02	9th Presidential Authorization signed
[redacted]	[redacted]
12-Aug-02	NSA briefs FISC Presiding Judge Kollar-Kotelly at the White House
13-Aug-02	NSA Inspector General (IG) cleared for the PSP
10-Sep-02	10th Presidential Authorization signed
11-Sep-02	NSA GC, Deputy General Counsel (GC), Associate GC for Operations, and IG meet to discuss PSP oversight
[redacted]	[redacted]
18-Sep-02	1st NSA Due Diligence Meeting
30-Sep-02	Chair HPSCI visits NSA for briefing
[redacted]	[redacted]
15-Oct-02	11th Presidential Authorization signed
[redacted]	[redacted]
18-Nov-02	12th Presidential Authorization signed
[redacted]	[redacted]
16-Dec-02	NSA IG advises General Hayden to issue "Delegation of Authority Letters" to "units that administer the project"
2003	
8-Jan-03	13th Presidential Authorization signed
[redacted]	[redacted]

Date	Event
[redacted]	[redacted]
13-Jan-03	FBI Director visits NSA for briefing
29-Jan-03	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
7-Feb-03	14th Presidential Authorization signed
[redacted]	[redacted]
4-Mar-03	General Hayden issues first Delegation of Authority letter to key Signals Intelligence (SIGINT) Directorate operational personnel
[redacted]	
17-Mar-03	15th Presidential Authorization signed
[redacted]	[redacted]
22-Apr-03	16th Presidential Authorization signed
[redacted]	[redacted]
11-Jun-03	17th Presidential Authorization signed
[redacted]	[redacted]
14-Jul-03	18th Presidential Authorization signed
[redacted]	[redacted]
17-Jul-03	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
[redacted]	[redacted]
10-Sep-03	19th Presidential Authorization signed
[redacted]	[redacted]

Date	Event
8-Oct-03	NSA-FBI-CIA conference at NSA to discuss PSP operations and customer needs
15-Oct-03	**20th Presidential Authorization signed**
[redacted]	[redacted]
1-Dec-03	NSA IG announces a review of NSA PSP operations
8-Dec-03	NSA IG asks VP Counsel for access to PSP legal opinions and is told that a request should come from General Hayden
9-Dec-03	**21st Presidential Authorization signed**
9-Dec-03	IG memo asks General Hayden to ask VP Counsel's permission for NSA IG and GC to obtain copies of, or view, PSP legal justification
[redacted]	[redacted]
2004	
6-Jan-04	NSA briefing to DoJ Mr. Philbin, Mr. Goldsmith for Mr. Goldsmith's orientation to the PSP and other NSA Signals Intelligence efforts against terrorism
8-Jan-04	NSA and FBI [redacted] meet to discuss the PSP and recent changes at NSA
14-Jan-04	**22nd Presidential Authorization signed**
[redacted]	[redacted]
9-Mar-04	General Hayden briefs Director of Central Intelligence (DCI) on value of the PSP
10-Mar-04	General Hayden briefs White House Counsel and Chief of Staff, Deputy DCI, Deputy AG, and FBI Director on value of the PSP
10-Mar-04	General Hayden briefs Speaker of the House, Senate Majority and Minority leaders, House Minority Leader, Chairman and Ranking Member, HPSCI, and Chair and Vice Chair, SSCI
10-Mar-04	General Hayden briefs Secretary of Defense, DoD Principal Deputy GC
11-Mar-04	**23rd Presidential Authorization signed**
11-Mar-04	NSA IG and Acting GC discuss new Authorization signed by President's Counsel rather than the AG
11-Mar-04	NSA briefs House Majority Leader
[redacted]	[redacted]
12-Mar-04	General Hayden briefs House Majority Leader
19-Mar-04	**Revision to 23rd Presidential Authorization signed**
[redacted]	General Hayden sends letter to Assistant AG, Office of Legal Counsel (OLC) [redacted]

Date	Event
	[redacted]
2-Apr-04	**2nd Revision to 23rd Presidential Authorization signed**
4-Apr-04	General Hayden briefs DoD Principal Deputy GC
5-May-04	**24th Presidential Authorization signed**
	[redacted]
20-May-04	NSA briefs the Minority Leader of the Senate
	[redacted]
23-Jun-04	**25th Presidential Authorization signed**
	[redacted]
14-Jul-04	Initial PR/TT Order approved by FISC
9-Aug-04	**26th Presidential Authorization signed**
	[redacted]
23-Aug-04	General Hayden briefs National Security Advisor and Homeland Security Advisor
	[redacted]
17-Sep-04	**27th Presidential Authorization signed**
	[redacted]
23-Sep-04	Presidential "further direction" of 9 August 2004 expires
23-Sep-04	NSA briefs Chair, HPSCI
	[redacted]
17-Nov-04	**28th Presidential Authorization signed**
	[redacted]
2005	
5-Jan-05	NSA briefs National Security Advisor and White House Counsel
	[redacted]
11-Jan-05	**29th Presidential Authorization signed**

Date	Event
[redacted]	[redacted]
3-Feb-05	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
25-Feb-05	General Hayden briefs White House Counsel and Counsel to Deputy AG
1-Mar-05	**30th Presidential Authorization signed**
2-Mar-05	NSA briefs Senate Minority Leader
[redacted]	[redacted]
19-Apr-05	**31st Presidential Authorization signed**
[redacted]	[redacted]
22-Apr-05	General Hayden briefs Director of National Intelligence (DNI)
23-May-05	Two-level PSP clearance structure discontinued
1-Jun-05	Discussions to seek FISC orders to authorize content collection begin with DoJ OLC
14-Jun-05	**32nd Presidential Authorization signed**
[redacted]	[redacted]
26-Jul-05	33rd Presidential Authorization signed
[redacted]	[redacted]
3-Aug-05	Principal Deputy DNI Hayden briefs new NSA/CSS Director General Alexander on the PSP
10-Sep-05	**34th Presidential Authorization signed**
14-Sep-05	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
[redacted]	[redacted]
26-Oct-05	**35th Presidential Authorization signed**
[redacted]	[redacted]
13-Dec-05	**36th Presidential Authorization signed**
16-Dec-05	New York Times says that President secretly authorized NSA eavesdropping on Americans
[redacted]	[redacted]
20-Dec-05	DoD IG receives letter, signed by 39 Congressmen, requesting a review of the PSP. DoD IG faxes the letter to the NSA IG on 10 Jan 06
21-Dec-05	NSA briefs DNI

Date	Event
2006	
3-Jan-06	NSA IG and DoD IG discuss letter from 39 Congressmen requesting DoD IG review of the PSP
9-Jan-06	NSA briefs nine FISC judges and three FISC legal advisors
11-Jan-06	NSA briefs Speaker of the House, Senate Majority Leader, Chair of HPSCI, Chair and Vice Chair, SSCI
20-Jan-06	NSA briefs Senate Minority Leader, House Minority Leader, Chair SSCI, and Ranking Member HPSCI
[redacted]	[redacted]
27-Jan-06	**37th Presidential Authorization signed**
31-Jan-06	NSA briefs FISC Judge Scullin
[redacted]	[redacted]
11-Feb-06	NSA briefs Chair SSCI
16-Feb-06	NSA briefs Speaker of the House and Chair, HPSCI
28-Feb-06	NSA briefs Chair and Ranking Member, House Appropriations Subcommittee on Defense
[redacted]	[redacted]
3-Mar-06	NSA briefs Vice Chair, SSCI
9-Mar-06	NSA briefs Chair and Vice Chair, SSCI, and Members of SSCI Terrorist Surveillance Program (TSP) Subcommittee (Roberts, Rockefeller, Hatch, DeWine, Feinstein, Levin, Bond) with SSCI Minority and Majority Staff Directors, Senior Director for Legislative Affairs, National Security Counsel, VP, AG, White House Counsel, and VP Chief of Staff
10-Mar-06	NSA briefs Mr. Bond, Member, SSCI TSP Subcommittee
13-Mar-06	NSA briefs Chair, SSCI TSP Subcommittee, Members SSCI TSP Subcommittee (Roberts, Feinstein, and Hatch), SSCI Majority and Minority Staff Directors, and SSCI Counsel at NSA
14-Mar-06	NSA briefs Mr. DeWine, Member, SSCI TSP Subcommittee at NSA
21-Mar-06	**38th Presidential Authorization signed**
21-Mar-06	NSA briefs FISC Judge Bates
[redacted]	[redacted]
27-Mar-06	NSA briefs Mr. Levin, Member, SSCI TSP Subcommittee and Minority Staff Director at NSA
29-Mar-06	NSA briefs Chairman and Ranking Member HPSCI TSP Subcommittee, TSP Subcommittee Members (Hoekstra, Harman, McHugh, Rogers, Thornberry, Wilson, Davis, Holt, Cramer, Eshoo, and Boswell), Majority General Counsel, Staff Member, and Minority General Counsel

Date	Event
7-Apr-06	NSA briefs Chairman of the HPSCI TSP Subcommittee, HPSCI TSP Subcommittee Members (Hoekstra, McHugh, Rogers, Thornberry, Wilson, and Holt), Majority General Counsel, Staff Member, and Minority General Counsel at NSA
[redacted]	[redacted]
28-Apr-06	NSA briefs Ranking Member, HPSCI TSP Subcommittee, Members of HPSCI TSP Subcommittee (Harman, Wilson, and Eshoo), Majority General Counsel, Staff Member, and Minority General Counsel at NSA
[redacted]	
11-May-06	NSA briefs Chair and Ranking Member House Appropriations Committee Defense Subcommittee
16-May-06	**39th Presidential Authorization signed**
17-May-06	Chair SSCI, Members, SSCI (Roberts, Hagel, Mikulski, Snowe, DeWine, Bayh, Chambliss, Lott, Bond, Levin, Feingold, Feinstein, Wyden, Warner), SSCI Staff Member, SSCI Majority Staff Director, and SSCI Counsel
17-May-06	HPSCI Chair, HPSCI Members (Hoekstra, Harman, Wilson, Eshoo, Rogers, Thornberry, Holt, Boswell, Cramer, LaHood, Everett, Gallegly, Davis, Tiahrt, Reyes, Ruppersberger, and Tierney), Majority General Counsel, Staff Director, and Minority General Counsel
[redacted]	[redacted]
24-May-06	First Business Records Order approved by the FISC
5-Jun-06	NSA briefs Ms. Feingold, SSCI Member at NSA
7-Jun-06	NSA briefs Ranking Member, Senate Defense Appropriations Subcommittee, and SSCI Staff Director
7-Jun-06	NSA briefs President's Privacy and Civil Liberties Oversight Board
9-Jun-06	NSA briefs Chair, SSCI, SSCI Members (Mikulski, Wyden, and Hagel), SSCI Minority Staff Director, SSCI Counsel, and SSCI Staff Director
15-Jun-06	NSA briefs Chair, SSCI and SSCI Members (Roberts, Mikulski, Feingold, Bayh, Snowe, Hatch, Lott, and Bond), and Minority Staff Director
26-Jun-06	NSA briefs Chair, Senate Defense Appropriations Subcommittee, and House Minority Leader
30-Jun-06	NSA briefs Mr. Bayh, SSCI Member at NSA
6-Jul-06	**40th Presidential Authorization signed**
[redacted]	[redacted]
10-Jul-06	NSA briefs Ms. Snowe, SSCI Member and SSCI Counsel at NSA
18-Jul-06	NSA briefs Mr. Chambliss, SSCI Member at NSA
[redacted]	
6-Sep-06	**41st Presidential Authorization signed**
[redacted]	[redacted]

Date	Event
[redacted]	[redacted]
24-Oct-06	**42nd Presidential Authorization signed**
[redacted]	[redacted]
20-Nov-06	NSA briefs President's Privacy and Civil Liberties Oversight Board
8-Dec-06	**43rd and final Presidential Authorization signed**
[redacted]	[redacted]

2007

10-Jan-07	Content orders approved by the FISC
17-Jan-07	AG letter to Congress: Presidential program brought under the FISC
1-Feb-07	NSA briefs President's Privacy and Civil Liberties Oversight Board
1-Feb-07	Presidential Authorization expires

~~(TS//STLW//SI//OC/NF)~~

This page intentionally left blank.

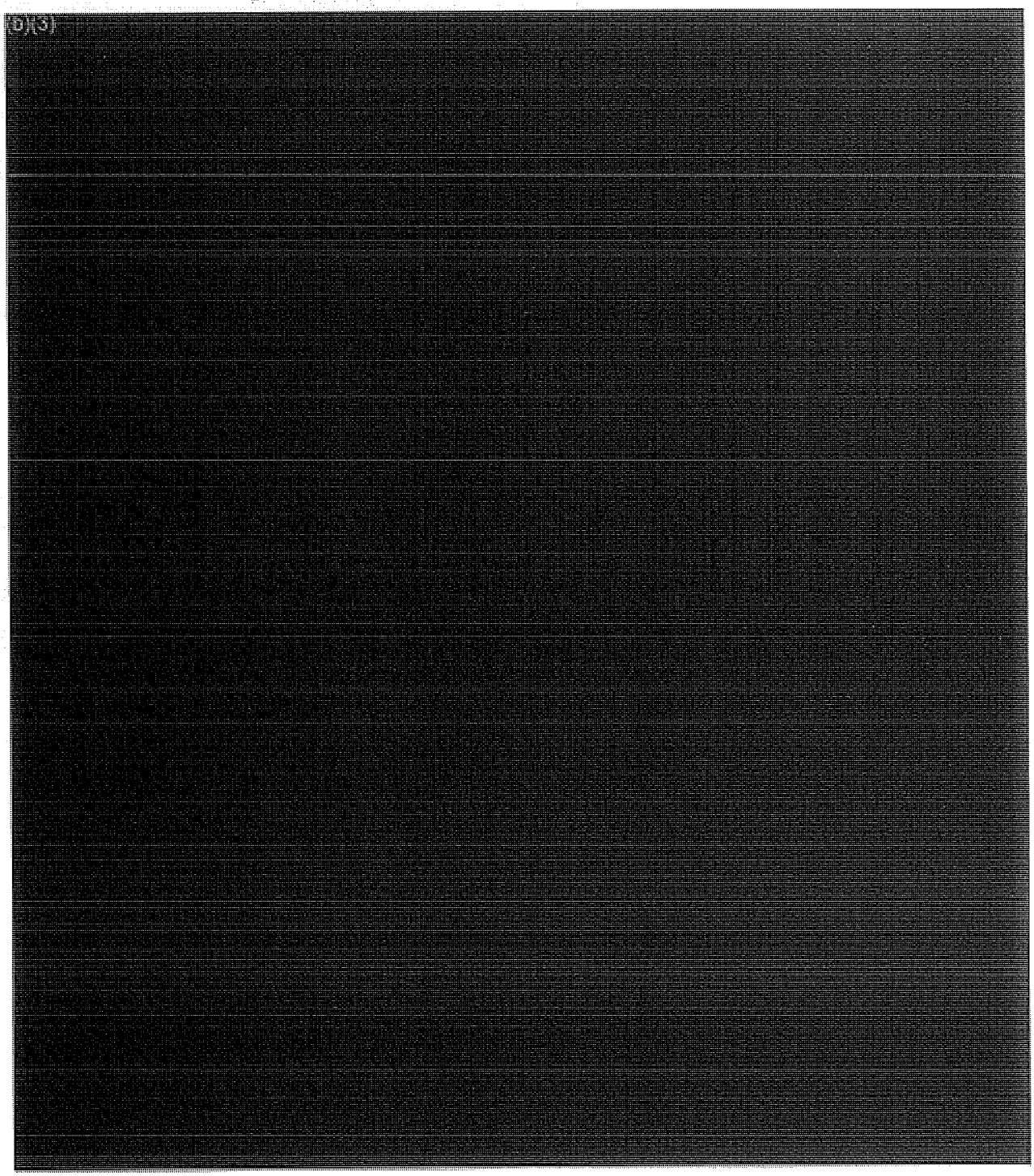
APPENDIX D

(U) Cumulative Number of Clearances for the President's Surveillance Program

This page intentionally left blank.

(U) Cumulative Number of Clearances for the President's Surveillance Program[4]

(b)(3)



This page intentionally left blank.

APPENDIX E

(U) NSA Office of the Inspector General Reports on the President's Surveillance Program and Related Activities

This page intentionally left blank.

(U) NSA Office of the Inspector General Reports on the President's Surveillance Program and Related Activities

~~(TS//SI//NF)~~ This appendix lists and describes OIG investigation and review reports of activity conducted under the PSP, also referred to as the STELLARWIND Program, and related activities such as the Pen Register Trap and Trace (PR/TT) Order and the Business Records Order. These reports are limited to activity conducted between 4 October 2001 and 17 January 2007.

(U) OIG Investigations

[redacted]

(U) Report of Investigation of Two Violations

~~(S//NF)~~ On [redacted] the OIG issued a report on what it believed to be the first two violations of Authorization, both of which were unintentional.

~~(TS//STLW//SI//OC/NF)~~ The first incident occurred on [redacted] An NSA analyst misguidedly used PSP authority to collect communications between [redacted] These communications were foreign within the meaning of the Authorization, but they were not terrorist related, [redacted]

~~(TS//STLW//SI//OC/NF)~~ The second incident occurred on [redacted] when NSA inappropriately performed contact chaining on [redacted] This query was requested by an FBI official during the investigation of [redacted]

~~(S//NF)~~ NSA OIG found that in neither incident had NSA personnel acted with intent to disregard their authority.

Both incidents occurred, at least in part, because early in the Program the terms of the Authorization were so closely held that few, if any, operational personnel working under the Authority were permitted to see the Authorization or its operative provisions. It was unreasonable to hold persons accountable for violating an order that they had not seen, when the order was too complex to be easily committed to memory. Accordingly, the OIG did not recommend disciplinary action, but did recommend that the NSA Director issue formal written delegations of authority to the Signals Intelligence Director and specified subordinates so that personnel working the Program would know the precise terms of the Authorization. Management concurred with the recommendations and made appropriate notifications.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008.

[redacted] ~~(TS//SI//NF)~~ ***Violations of Court Orders in [redacted] Foreign Intelligence Surveillance Court***

~~(TS//STLW//SI//OC/NF)~~ On 14 July 2004 [redacted] The Order permitted NSA to collect Internet metadata under the pen register/trap-and-trace provisions of the FISA (§§ 1841-1846). The authority to collect Internet metadata under the Order [redacted] Material acquired under the Order continued to be protected in PSP channels.

~~(TS//STLW//SI//OC/NF)~~ On [redacted] NSA OIG issued a report on an investigation of a management breakdown that had resulted in unintentional filtering violations of the FISC Order. The Order permitted NSA to collect Internet metadata from communications involving [redacted] The violations occurred because NSA [redacted] However, no violations resulted from the collection of domestic communications. An NSA collection manager discovered the violations on [redacted]. The following day, the questionable collection was stopped and reported to the OIG and the OGC. With the exception of [redacted] the OIG

found no reason to believe that any violations resulted in the collection of U.S. person information. The OIG reserved judgment on [redacted] The OIG evaluation of responsibility for the incident led directly to the replacement of the Program Manager and to changes in Program management, leadership, and chain of command.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

[redacted]

~~(TS//SI//NF)~~ Supplemental Report on Violations of Court Orders in [redacted]

~~(TS//STLW//SI//OC/NF)~~ A follow-up investigation of the questionable [redacted] revealed no additional violations. On [redacted] the NSA OIG issued a report detailing its examination of [redacted] that the OIG suspected might not have originated or terminated outside the United States. [redacted] All but [redacted] messages could have been associated with a foreign sender or recipient. [redacted] None of the [redacted] messages had been intentionally collected, none had been analyzed, and none had been reported outside NSA.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008.

(U) OIG Reviews

14 May 2004 ***(U) Need for Documentation and Development of Key Processes (ST-04-0024)***

~~(TS//SI//NF)~~ This OIG report concluded that a continuing deficiency in clear, written procedures governing the collection, processing, and dissemination of PSP material created undue risk of unintentional violations of the Authorization. The report noted that Program officials had

made progress in addressing some of these deficiencies, but found that processes had not been fully documented in the form of management directives, administrative policies, or operating manuals. The NSA OIG recommended that Program officials formally adopt rigorous, written operating procedures for the following key processes:

- Approvals for content collection by the appropriate named officials
- Reporting of violations of the Authority, similar to procedures for documenting violations of Legal Compliance and Minimization Procedures[5]
- Evaluation of dual FISA and PSP content collection
- Systematic identification and evaluation of telephone numbers and Internet identifiers for detasking.[6]

(U//~~FOUO~~) Corrective action was taken in response to the four recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 06 and HPSCI on 2 January 2008.

13 Sep 2004 ***~~(S//NF)~~ Need for Increased Attention to Security-Related Aspects of the STELLARWIND Program (ST-04-0025)***

(U//~~FOUO~~) This OIG report disclosed weaknesses in Program security. The Program was particularly vulnerable to exposure because it involved numerous organizations inside and outside NSA.

(U//~~FOUO~~) While the Program Manager placed a strong emphasis on personnel security, he did not take a proactive and strategic approach to physical and operational security. In particular, better use of the Program Security Officer would have helped to improve special security practices for handling Program material and strengthen operations security (OPSEC).

(U//~~FOUO~~) The Program Manager and the Associate Director for Security and Counterintelligence concurred with the findings and implemented corrective measures. In particular,

---

[5](U) U.S. Signals Intelligence Directive 18 or "USSID SP0018" (as of 27 July 2003).
[6](~~TS//SI//NF~~) [redacted]

the Staff Security Officer was freed from other responsibilities and took a more active and effective role in Program security. Management did not conduct a formal OPSEC survey as recommended; however, steps taken by management to implement OPSEC practices met the intent of the original recommendation.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008.

21 Nov 2005 ***~~(TS//SI//NF)~~ Review of the Tasking Process for STELLARWIND U.S. Content Collection (ST-04-0026)***

~~(TS//STLW//SI//OC/NF)~~ This report identified material weaknesses in the tasking and detasking process under the PSP. The process to task and detask telephone numbers for content collection under the Program was inherently fragile because it was based on e-mail exchanges and was not automated or monitored.

~~(TS//STLW//SI//OC/NF)~~ The OIG examined [redacted] telephone numbers and Internet identifiers approved for content collection on the date in November 2004 when the audit began and identified the following types of errors:

- [redacted] involved under-collection; identifiers were not put on collection quickly enough or were not put on collection until the OIG discovered the errors.
- [redacted] involved unauthorized collection caused by a typographical error.
- [redacted] involved over-collection; they were not removed from collection quickly enough.
- [redacted] record-keeping errors in the Program's tracking database

~~(TS//STLW//SI//OC/NF)~~ In the [redacted] of unauthorized collection caused by a typographical error, NSA personnel did not review the collected information before destroying it, nor did NSA issue any report based on, or otherwise disseminate, any information from the [redacted] of untimely detasking. However, without a robust and reliable collection and tracking process, NSA increased its risk of unintentionally violating the Authorization. NSA also increased the risk of missing

valuable foreign intelligence by failing to task telephone numbers and Internet identifiers in a timely manner.

(U//~~FOUO~~) NSA OIG recommended that all errors be swiftly resolved, that specific procedures be adopted to prevent recurrences, and that identifiers tasked for collection be promptly reconciled with identifiers approved for tasking, and repeated every 90 days. Management implemented the recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

31 May 2006 ***~~(TS//SI//NF)~~ Review of Compliance with Authorization Requirements for STELLARWIND U.S. Content Collection (ST-04-0027)***

~~(TS//STLW//SI//OC/NF)~~ This report determined that, based on a statistical sample, Program officials were adhering to the terms of the Authorization and the Director's delegation thereunder; that tasking was appropriately approved and duly recorded under the Authorization; and that tasking was justified as linked to al-Qa'ida or affiliates of al-Qa'ida. The report recommended improvements in record-keeping practices.

~~(S//NF)~~ Due to a lack of sufficient and reliable data, the NSA OIG could not reach a conclusion on the tasking approval process for two PSP-related collection programs. The OIG recommended that management responsible for the affected programs, design and implement a tasking and tracking process to allow managers to audit, assess timeliness, and validate the sequencing of tasking activities. Management agreed to install automated tracking of tasking and detasking.

~~(TS//SI//NF)~~ Although the collection architecture was designed to produce one-end-foreign communications, inadvertent collection of domestic communications occurred and was addressed. The OIG recommended changes in management reporting to improve the tracking and resolution of inadvertent collection issues.

(U//~~FOUO~~) Corrective action has been completed for one of the two recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

11 Jul 2006 ***~~(TS//SI//NF)~~ Supplemental Report to Review of Compliance with Authorization Requirements for STELLARWIND U.S. Content Collection (ST-04-0027.01)***

~~(TS//STLW//SI//OC/NF)~~ After issuing the original report, the NSA OIG conducted further research to determine whether Program officials were approving content tasking requests based solely on metadata analysis. Using the statistical sample in the original audit, the OIG found no instances of metadata analysis as the sole justification for content tasking. In all cases tested, there was corroborating evidence to support the tasking decision.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008.

5 Sep 2006 ***~~(TS//SI//NF)~~ Report on the Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance Court Order: Telephony Business Records (ST-06-0018)***

~~(TS//STLW//SI//OC/NF)~~ On 24 May 2006, the telephony metadata portion of the PSP was transferred to FISC Order BR-06-05, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from* [Telecommunications Providers] *Relating to* [redacted] The Order authorized NSA to collect and retain telephony metadata to protect against international terrorism and to process and disseminate this data regarding [redacted]

~~(TS//SI//NF)~~ On 10 July 2006, in a memorandum with the subject *FISA Court Order: Telephony Business Records (ST-06-0018)*, the NSA OIG issued "a report to the Director of NSA 45 days after the initiation of the activity [permitted by the Order] assessing the adequacy of the management controls for the processing and dissemination of U.S. person information." This report was issued with the Office of the General Counsel's concurrence as mandated by the Order.

~~(TS//SI//NF)~~ The "*Report on the Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance*

Court Order: Telephony Business Records (ST-06-0018)," 5 September 2006, provided the details of the findings of the 10 July memorandum and made formal recommendations to management.

~~(TS//SI//NF)~~ Management controls governing the processing, dissemination, data security, and oversight of telephony metadata and U.S. person information obtained under the Order were adequate and in several aspects exceeded the terms of the Order. However, due to the risk associated with the collection and processing of telephony metadata involving U.S. person information, the NSA OIG recommended three additional controls regarding collection procedures, reconciliation of audit logs, and segregation of duties.

~~(TS//SI//NF)~~ Collection Procedures

~~(TS//SI//NF)~~ During an OIG review of collection procedures, Program management discovered that NSA was obtaining [redacted] data that might not have been in keeping with the Order: [redacted] OGC advised that [redacted] data should have been suppressed from the incoming data flow. Immediately, management blocked the data from analysts' view. Further, working with the providers, Program management completed suppression of the suspect data on 11 October 2006 and agreed to implement additional procedures to prevent the collection of unauthorized data.

~~(TS//SI//NF)~~ Reconciliation of Audit Logs

~~(TS//SI//NF)~~ Management controls were not in place to verify that telephone numbers approved for querying were the only numbers queried. Although audit logs documented the queries of the archived metadata, the logs were not in a usable format, and Program management did not routinely use them to audit telephone numbers queried. Management concurred with the recommendation to conduct periodic reconciliations; however, action was contingent on the approval of a Program management request for two additional computer Programmers.

[redacted]

~~(C//NF)~~ Lack of Segregation of Duties

~~(C//NF)~~ The seven individuals with the authority to approve queries also had the ability to conduct queries under the Order. Standard internal control practices require that key duties and responsibilities be divided among different people to reduce the risk of error and fraud. Although Program management concurred with the finding, it could not implement the recommendation due to staffing and operational needs. As an alternative, Program management agreed to develop a process to monitor independently the queries of the seven individuals. This action plan was contingent on the development of usable audit logs recommended above.

(U//~~FOUO~~) Corrective action has been completed for one of the three recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008.

20 Dec 2006

~~(S//NF)~~ Summary of OIG Oversight 2001-2006 STELLARWIND Program Activities (ST-07-0011)

~~(S//NF)~~ On 20 December 2006, the OIG issued a report summarizing OIG's oversight of the STELLARWIND Program after five years of implementation.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

[redacted]

~~(TS//SI//NF)~~ Assessment of Management Controls to Implement the FISC Order Authorizing NSA to Collect Information Using Pen Register and Trap and Trace Devices (ST-06-0020)

~~(TS//SI//NF)~~ On [redacted] the OIG reported that the management controls governing the collection, dissemination, and data security of electronic communications metadata and U.S. person information obtained under the FISC Order authorizing NSA to collect Internet metadata using PR/TT devices were adequate and in several aspects exceeded the terms of the Order. Due to the risk associated with the processing of electronic communications metadata involving U.S. person information, additional controls were needed for processing and monitoring queries made against PR/TT data, documenting

ST-09-0002 ~~*TOP SECRET//STLW//COMINT//ORCON/NOFORN*~~

oversight activities, and providing annual refresher training on the terms of the Order.

(U//~~FOUO~~) Corrective action has been completed for two of the six recommendations.

(U//~~FOUO~~) This report was sent to SSCI on [redacted] and HPSCI on [redacted]

5 Jul 2007 ***~~(TS//SI//NF)~~ Domestic Selector Tasking Justification Review (ST-07-0017)***

(U//~~FOUO~~) The OIG conducted this review to determine whether tasking justification statements were supported with intelligence information consistent with sources cited in the justifications. The OIG identified some justifications containing errors, but there was no pattern of errors or exaggeration of facts or intentional misstatements.

(U//~~FOUO~~) This report was sent to SSCI on 28 January 2008 and HPSCI on 28 January 2008.

30 June 2008 ***~~(TS//SI//NF)~~ Advisory Report on the Adequacy of STELLARWIND Decompartmentation Plans (ST-08-0018)***

~~(TS//SI//NF)~~ At the request of the SID Program Manager for CT Special Projects, the OIG assessed the adequacy of NSA's plans to remove data from the STELLARWIND compartment, as authorized by the Director of National Intelligence. On 30 June 2008, the OIG reported that NSA management had a solid foundation of planning for decompartmentation. In particular, the content, communication, and assignment of supporting plans were adequate to provide reasonable assurance of successfully removing data from the STELLARWIND compartment, while complying with laws and authorities. Management was also diligent in assessing the scope and complexity of this undertaking. Although the OIG made no formal recommendations, it suggested improvements to develop more detailed plans, set firm milestones, and establish a feedback system to ensure that plans were successfully implemented.

(U//~~FOUO~~) This report was not sent to SSCI or HPSCI.

APPENDIX F

(U) Presidential Notifications

This page intentionally left blank.

(U) Presidential Notifications

~~(TS//STLW//SI//OC/NF)~~ Executive Orders 12333 and 12863 require intelligence agencies to report to the President, through the President's Intelligence Oversight Board, activities they have reason to believe may be unlawful or contrary to executive order or presidential directive. Knowing that Board members were not cleared, however, the NSA Director or Deputy Director reported the following violations of the Presidential Authorization and related authorities to the President through his Counsel, rather than through the Board. Each notification was approved if not actually drafted by OIG. Some of the notifications were not the subject of the OIG reviews or investigations discussed in Appendix E.

(U) Date	(U) Summary of Notification
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes violations regarding (1) the [redacted] and (2) [redacted]
[redacted]	[redacted]
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes a delay of about 90 days in detasking a telephone number [redacted]
[redacted]	~~(TS//SI//NF)~~ Describes the investigation mentioned above regarding metadata collection violations that occurred under FISA Court Order *In Re* [redacted] FISA Court [redacted] The complete OIG report was issued [redacted]
[redacted]	~~(TS//SI//NF)~~ Describes [redacted] instances in which cleared NSA analysts mistakenly accessed data [redacted] In one instance, a report based on such data went out, but it was not cancelled because the same information was available elsewhere. In the other [redacted] instances, no reports were issued. [redacted]

(U) Date	(U) Summary of Notification
	[redacted]
[redacted]	(~~TS//STLW//SI//OC/NF~~) Describes one instance of inadvertent collection of a call with both ends in the U.S. – a fact that could not have been known until it was listened to because [redacted] showed the call as having a foreign origin. [redacted]
[redacted]	(~~TS//SI//NF~~) Describes three incidents: The first involved a one-digit typo resulting in one incorrectly tasked number. The second involved a number improperly tasked for metadata analysis. The operator discovered it almost immediately and promptly removed it from tasking. The third involved [redacted] numbers that were not detasked in a timely fashion.
2 Aug 2005 [redacted]	(~~TS//SI//NF~~) Describes the evolving [redacted] a practice that may have resulted in over-collection. The notification refers to NSA's work in developing more rigorous [redacted]
[redacted]	(~~TS//STLW//SI//OC/NF~~) Describes an incident in which bulk telephony metadata was actively collected in spite [redacted] At that time NSA limited collection of bulk telephone records to [redacted] as permitted by statute. The collection resulted when [redacted] The error was not discovered for 18 months. (~~TS//STLW//SI//OC/NF~~) Although most of the metadata improperly collected was also properly acquired [redacted] pursuant to statute, the dataflow was terminated immediately upon discovery. Also, because the improperly collected metadata had been forwarded to non-STELLARWIND databases, the Agency removed non-compliant metadata from all affected databases, including those in which STELLARWIND data is normally stored.

(U) Date	(U) Summary of Notification
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes an incident in which an [redacted] This resulted [redacted] of non-target data. The error was discovered within hours, when personnel responsible for monitoring [redacted] The error was corrected, and all inadvertently collected records were deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case, [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case, [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes an instance where a [redacted] Although no reports were generated, and there was no evidence that U.S.-to-U.S. communications were collected, we could not certify that the files were all one-end foreign without reviewing [redacted] The [redacted] files were deleted, and procedures used by [redacted] were being reviewed. ~~(TS//STLW//SI//OC/NF)~~ A second incident was reported in which a typographical error resulted in contact chaining on a U.S. telephone number with no [redacted] affiliation. The telephone number was rechecked, and the error was corrected.

This page intentionally left blank.

APPENDIX G

(U) United States Signals Intelligence Directive SP0018, Legal Compliance and Minimization Procedures

This page intentionally left blank.

~~SECRET~~

AUTHORIZED REPRODUCTION NUMBER 00R0043

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

Fort George G. Meade, Maryland

UNITED STATES
SIGNALS INTELLIGENCE
DIRECTIVE
18

27 July 1993

INCLUDES CHANGES 1 and 2

See Letter of Promulgation for instructions on reproduction or release of this document.

~~OPR: D2~~
~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

This page intentionally left blank.

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
Fort George G. Meade, Maryland

27 July 1993

UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE

(USSID)

18

LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES ~~(FOUO)~~

LETTER OF PROMULGATION

(U) This USSID prescribes policies and procedures and assigns responsibilities to ensure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights of U.S. persons.

(U) This USSID has been completely rewritten to make it shorter and easier to understand. It constitutes a summary of the laws and regulations directly affecting USSS operations. All USSS personnel who collect, process, retain, or disseminate information to, from, or about U.S. persons or persons in the United States must be familiar with its contents.

~~(FOUO)~~ This USSID supersedes USSID 18, and USSID 18, Annex A (distributed separately to selected recipients), both of which are dated 20 October 1980, and must now be destroyed. Notify DIRNSA/CHCSS (USSID Manager) if this edition of USSID 18 is destroyed because of an emergency action; otherwise, request approval from DIRNSA/CHCSS before destroying this USSID.

~~(FOUO)~~ Release or exposure of this document to contractors and consultants without approval from the USSID Manager is prohibited. Instructions applicable to release or exposure of USSID to contractors and consultants may be found in USSID 19.

~~(FOUO)~~ Questions and comments concerning this USSID should be addressed to the Office of the General Counsel, NSA/CSS, NSTS 963-3121 or [redacted]

J.M.McCONNELL
Vice Admiral, U.S. Navy
Director

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

This page intentionally left blank.

USSID 18
27 July 1993

CHANGE REGISTER

No	Date	CHANGE Authority (Msg Cite/DTG, Hard Copy (HC))	ENTERED Date	By
1	28OCT97	HARDCOPY CHANGE	29OCT97	RS
2	11Dec98	P0211–0307–98, 111600Z Dec 98	11Dec98	WF
2	11Dec98	P0211–0309–98, 111640Z Dec 98 (correction to above)	11Dec98	WF

This page intentionally left blank.

TABLE OF CONTENTS

SECTION 1 – PREFACE 1

SECTION 2 – REFERENCES 1

SECTION 3 – POLICY 2

SECTION 4 – COLLECTION 2

4.1. Communications to, from or About U.S. Persons and [redacted] 2

a. Foreign Intelligence Surveillance Court Approval 2

b. Attorney General Approval 2

c. DIRNSA/CHCSS Approval 2

d. Emergency Situations 3

e. Annual Reports 4

4.2. [redacted] 4

4.3. Incidental Acquisition of U.S. Person Information 4

4.4. Nonresident Alien Targets Entering the United States 5

4.5. U.S. Person Targets Entering the United States 5

4.6. Requests to Target U.S. Persons 5

4.7. Direction Finding 5

4.8. Distress Signals 5

4.9. COMSEC Monitoring and Security Testing of Automated Information Systems 6

SECTION 5 – PROCESSING 6

5.1. Use of Selection Terms During Processing 6

5.2. Annual Review by DDO 6

5.3. Forwarding of Intercepted Material 6

5.4. Nonforeign Communications 7

a. Communications between Persons in the United States 7

b. Communications between U.S. Persons 7

c. Communications Involving an Officer or Employee of the U.S. Government 7

d. Exceptions 7

5.5. Radio Communications with a Terminal in the United States 7

SECTION 6 – RETENTION 8

6.1. Retention of Communications to, from, or About U.S. Persons 8

a. Unenciphered Communications; and Communications Necessary to Maintain Technical Data Bases for Cryptanalytic or Traffic Analytic Purposes 8

b. Communications Which Could be Disseminated Under Section 7 8

6.2. Access 8

SECTION 7 – DISSEMINATION 8

7.1. Focus of SIGINT Reports 8

7.2. Dissemination of U.S. Person Identities 9

a. Consent 9

b. Publicly Available Information 9

c. Information Necessary to Understand or Access 9

7.3. Approval Authorities 10

a. DIRNSA/CHCSS 10

b. Field Units 10

c. DDO and Designees 10

7.4. Privileged Communications and Criminal Activity 10

7.5. Improper Dissemination 10

SECTION 8 – RESPONSIBILITIES 11

8.1. Inspector General 11

8.2. General Counsel 11

8.3. Deputy Director for Operations 12

8.4. All Elements of the USSS 12

SECTION 9 – DEFINITIONS 12

ANNEX A – PROCEDURES IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (U) A/1

APPENDIX 1 – STANDARIZED MINIMIZATION PROCEDURES FOR NSA ELECTRONIC SURVEILLANCES A–1/1

ANNEX B – OPERATIONAL ASSISTANCE TO THE FEDERAL BUREAU OF INVESTIGATION (U) B/1

ANNEX C – SIGNALS INTELLIGENCE SUPPORT TO U.S. AND ALLIED MILITARY EXERCISE COMMAND AUTHORITIES (U) C/1

ANNEX D – TESTING OF ELECTRONIC EQUIPMENT (U) D/1

ANNEX E – SEARCH AND DEVELOPMENT OPERATIONS (U) E/1

ANNEX F – ILLICIT COMMUNICATIONS ~~(C)~~ F/1

ANNEX G – TRAINING OF PERSONNEL IN THE OPERATION AND USE OF SIGINT COLLECTION AND OTHER SURVEILLANCE EQUIPMENT (U) G/1

ANNEX H – CONSENT FORMS (U) H/1

ANNEX I – FORM FOR CERTIFICATION OF OPENLY-ACKNOWLEDGED ENTITIES ~~(S-CCO)~~ I/1

ANNEX J – PROCEDURES FOR MONITORING RADIO COMMUNICATIONS OF SUSPECTED INTERNATIONAL NARCOTICS TRAFFICKERS ~~(S-CCO)~~ (Issued separately to selected recipients) J/1

ANNEX K – [redacted] K/1

This page intentionally left blank.

27 July 1993

USSID 18

LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES (U)

SECTION 1 – PREFACE

1.1. (U) The Fourth Amendment to the United States Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government. The Supreme Court has ruled that the interception of electronic communications is a search and seizure within the meaning of the Fourth Amendment. It is therefore mandatory that signals intelligence (SIGINT) operations be conducted pursuant to procedures which meet the reasonableness requirements of the Fourth Amendment.

1.2. (U) In determining whether United States SIGINT System (USSS) operations are "reasonable," it is necessary to balance the U.S. Government's need for foreign intelligence information and the privacy interests of persons protected by the Fourth Amendment. Striking that balance has consumed much time and effort by all branches of the United States Government. The results of that effort are reflected in the references listed in Section 2 below. Together, these references require the minimization of U.S. person information collected, processed, retained or disseminated by the USSS. The purpose of this document is to implement these minimization requirements.

1.3. (U) Several themes run throughout this USSID. The most important is that intelligence operations and the protection of constitutional rights are not incompatible. It is not necessary to deny legitimate foreign intelligence collection or suppress legitimate foreign intelligence information to protect the Fourth Amendment rights of U.S. persons.

1.4. (U) Finally, these minimization procedures implement the constitutional principle of "reasonableness" by giving different categories of individuals and entities different levels of protection. These levels range from the stringent protection accorded U.S. citizens and permanent resident aliens in the United States to provisions relating to foreign diplomats in the U.S. These differences reflect yet another main theme of these procedures, that is, that the focus of all foreign intelligence operations is on foreign entities and persons.

SECTION 2 – REFERENCES

2.1. (U) References

a. 50 U.S.C. 1801, et seq., Foreign Intelligence Surveillance Act (FISA) of 1978, Public Law No. 95-511.

b. Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981.

c. DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," dated 25 April 1988.

d. NSA/CSS Directive No. 10-30, "Procedures Governing Activities of NSA/CSS that Affect U.S. Persons," dated 20 September 1990.

SECTION 3 – POLICY

3.1. (U) The policy of the USSS is to TARGET or COLLECT only FOREIGN COMMUNICATIONS. The USSS will not intentionally COLLECT communications to, from or about U.S. PERSONS or persons or entities in the U.S. except as set forth in this USSID. If the USSS inadvertently COLLECTS such communications, it will process, retain and disseminate them only in accordance with this USSID.

SECTION 4 – COLLECTION

4.1. ~~(S-CCO)~~ Communications which are known to be to, from or about a U.S. PERSON [redacted] will not be intentionally intercepted, or selected through the use of a SELECTION TERM, except in the following instances:

a. With the approval of the United States Foreign Intelligence Surveillance Court under the conditions outlined in Annex A of this USSID.

b. With the approval of the Attorney General of the United States, if:

(1) The COLLECTION is directed against the following:

(a) Communications to or from U.S. PERSONS outside the UNITED STATES, or

(b) International communications to, from, [redacted], or

(c) Communications which are not to or from but merely about U.S. PERSONS (wherever located).

(2) The person is an AGENT OF A FOREIGN POWER, and

(3) The purpose of the COLLECTION is to acquire significant FOREIGN INTELLIGENCE information.

c. With the approval of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), so long as the COLLECTION need not be approved by the Foreign Intelligence Surveillance Court or the Attorney General, and

(1) The person has CONSENTED to the COLLECTION by executing one of the CONSENT forms contained in Annex H, or

* Capitalized words in Sections 3 through 9 are defined terms in Section 9.

(2) The person is reasonably believed to be held captive by a FOREIGN POWER or group engaged in INTERNATIONAL TERRORISM, or

(3) The TARGETED [redacted] and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex I, or

(4) The COLLECTION is directed against [redacted] between a U.S. PERSON in the UNITED STATES and a foreign entity outside the UNITED STATES, the TARGET is the foreign entity, and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex K, or

(5) Technical devices (e.g. [redacted]) are employed to limit acquisition by the USSS to communications to or from the TARGET or to specific forms of communications used by the TARGET (e.g., [redacted] and the COLLECTION is directed against [redacted] voice and facsimile communications with one COMMUNICANT in the UNITED STATES, and the TARGET of the COLLECTION is [redacted]:

(a) A non-U.S. PERSON located outside the UNITED STATES [redacted]

(b) [redacted]

(6) Copies of approvals granted by the DIRNSA/CHCSS under these provisions will be retained in the Office of General Counsel for review by the Attorney General.

d. Emergency Situations.

(1) In emergency situations, DIRNSA/CHCSS may authorize the COLLECTION of information to, from, or about a U.S. PERSON who is outside the UNITED STATES when securing the prior approval of the Attorney General is not practical because:

(a) The time required to obtain such approval would result in the loss of significant FOREIGN INTELLIGENCE and would cause substantial harm to the national security.

(b) A person's life or physical safety is reasonably believed to be in immediate danger.

(c) The physical security of a defense installation or government property is reasonably believed to be in immediate danger.

(2) In those cases where the DIRNSA/CHCSS authorizes emergency COLLECTION, except for actions taken under paragraph d.(1)(b) above, DIRNSA/CHCSS shall find that there is probable cause that the TARGET meets one of the following criteria:

(a) A person who, for or on behalf of a FOREIGN POWER, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process),

sabotage, or INTERNATIONAL TERRORIST activities, or activities in preparation for INTERNATIONAL TERRORIST activities; or who conspires with, or knowingly aids and abets a person engaging in such activities.

(b) A person who is an officer or employee of a FOREIGN POWER.

(c) A person unlawfully acting for, or pursuant to the direction of, a FOREIGN POWER. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the FOREIGN POWER.

(d) A CORPORATION or other entity that is owned or controlled directly or indirectly by a FOREIGN POWER.

(e) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

(3) In all cases where emergency collection is authorized, the following steps shall be taken:

(a) The General Counsel will be notified immediately that the COLLECTION has started.

(b) The General Counsel will initiate immediate efforts to obtain Attorney General approval to continue the collection. If Attorney General approval is not obtained within seventy two hours, the COLLECTION will be terminated. If the Attorney General approves the COLLECTION, it may continue for the period specified in the approval.

e. Annual reports to the Attorney General are required for COLLECTION conducted under paragraphs 4.1.c.(3) and (4). Responsible analytic offices will provide such reports through the Deputy Director for Operations (DDO) and the General Counsel to the DIRNSA/CHCSS for transmittal to the Attorney General by 31 January of each year.

4.2. ~~(S-CCO)~~ [redacted]

a. [redacted]

b. [redacted]

4.3. (U) Incidental Acquisition of U.S. PERSON Information. Information to, from or about U.S. PERSONS acquired incidentally as a result of COLLECTION directed against appropriate FOREIGN INTELLIGENCE TARGETS may be retained and processed in accordance with Section 5 and Section 6 of this USSID.

4.4. ~~(S-CCO)~~ Nonresident Alien TARGETS Entering the UNITED STATES.

a. If the communications of a nonresident alien located abroad are being TARGETED and the USSS learns that the individual has entered the UNITED STATES, COLLECTION may continue for a period of 72 hours provided that the DIRNSA/CHCSS is advised immediately and:

(1) Immediate efforts are initiated to obtain Attorney General approval, or

(2) A determination is made within the 72 hour period that the [redacted]

b. If Attorney General approval is obtained, the COLLECTION may continue for the length of time specified in the approval.

c. If it is determined that [redacted] COLLECTION may continue at the discretion of the operational element.

d. If [redacted] or if Attorney General approval is not obtained within 72 hours, COLLECTION must be terminated [redacted] Attorney General approval is obtained, or the individual leaves the UNITED STATES.

4.5. ~~(C-CCO)~~ U.S. PERSON TARGETS Entering the UNITED STATES.

a. If communications to, from or about a U.S. PERSON located outside the UNITED STATES are being COLLECTED under Attorney General approval described in Section 4.1.b. above, the COLLECTION must stop when the USSS learns that the individual has entered the UNITED STATES.

b. While the individual is in the UNITED STATES, COLLECTION may be resumed only with the approval of the United States Foreign Intelligence Surveillance Court as described in Annex A.

4.6. ~~(S-CCO)~~ Requests to TARGET U.S. PERSONS. All proposals for COLLECTION against U.S. PERSONS, [redacted], must be submitted through the DDO and the General Counsel to the DIRNSA/CHCSS for review.

4.7. ~~(C-CCO)~~ Direction Finding. Use of direction finding solely to determine the location of a transmitter located outside of the UNITED STATES does not constitute ELECTRONIC SURVEILLANCE or COLLECTION even if directed at transmitters believed to be used by U.S. PERSONS. Unless COLLECTION of the communications is otherwise authorized under these procedures, the contents of communications to which a U.S. PERSON is a party monitored in the course of direction finding may only be used to identify the transmitter.

4.8. (U) Distress Signals. Distress signals may be intentionally collected, processed, retained, and disseminated without regard to the restrictions contained in this USSID.

4.9. (U) COMSEC Monitoring and Security Testing of Automated Information Systems. Monitoring for communications security purposes must be conducted with the consent of the person being monitored and in accordance with the procedures established in National Telecommunications and Information Systems Security Directive 600, Communications Security (COMSEC) Monitoring, dated 10 April 1990. Monitoring for

communications security purposes is not governed by this USSID. Intrusive security testing to assess security vulnerabilities in automated information systems likewise is not governed by this USSID.

SECTION 5 – PROCESSING

5.1. ~~(S-CCO)~~ Use of Selection Terms During Processing.
When a SELECTION TERM is intended to INTERCEPT a communication on the basis of the content of the communication, or because a communication is enciphered, rather than on the basis of the identity of the COMMUNICANT or the fact that the communication mentions a particular individual, the following rules apply:

a. No SELECTION TERM that is reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON (wherever located) [redacted] may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained by use of such SELECTION TERM.

b. No SELECTION TERM that has resulted in the INTERCEPTION of a significant number of communications to or from such persons or entities may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained.

c. SELECTION TERMS that have resulted or are reasonably likely to result in the INTERCEPTION of communications to or from such persons or entities shall be designed to defeat, to the greatest extent practicable under the circumstances, the INTERCEPTION of those communications which do not contain FOREIGN INTELLIGENCE.

5.2. ~~(S-CCO)~~ Annual Review by DDO.

a. All SELECTION TERMS that are reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON or terms that have resulted in the INTERCEPTION of a significant number of such communications shall be reviewed annually by the DDO or a designee.

b. The purpose of the review shall be to determine whether there is reason to believe that FOREIGN INTELLIGENCE will be obtained, or will continue to be obtained, by the use of these SELECTION TERMS.

c. A copy of the results of the review will be provided to the Inspector General and the General Counsel.

5.3. ~~(C-CCO)~~ Forwarding of Intercepted Material. FOREIGN COMMUNICATIONS collected by the USSS may be forwarded as intercepted to NSA, intermediate processing facilities, and collaborating centers.

5.4. ~~(S-CCO)~~ Nonforeign Communications.

a. Communications between persons in the UNITED STATES. Private radio communications solely between persons in the UNITED STATES inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be promptly destroyed unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

b. Communications between U.S. PERSONS. Communications solely between U.S. PERSONS will be treated as follows:

(1) Communications solely between U.S. PERSONS inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be destroyed upon recognition, if technically possible, except as provided in paragraph 5.4.d. below.

(2) Notwithstanding the preceding provision, cryptologic data (e.g., signal and encipherment information) and technical communications data (e.g., circuit usage) may be extracted and retained from those communications if necessary to:

(a) Establish or maintain intercept, or

(b) Minimize unwanted intercept, or

(c) Support cryptologic operations related to FOREIGN COMMUNICATIONS.

c. Communications Involving an Officer or Employee of the U.S. Government. Communications to or from any officer or employee of the U.S. Government, or any state or local government, will not be intentionally intercepted. Inadvertent INTERCEPTIONS of such communications (including those between foreign TARGETS and U.S. officials) will be treated as indicated in paragraphs 5.4.a. and b., above.

d. Exceptions: Notwithstanding the provisions of paragraphs 5.4.b. and c., the DIRNSA/CHCSS may waive the destruction requirement for international communications containing, inter alia, the following types of information:

(1) Significant FOREIGN INTELLIGENCE, or

(2) Evidence of a crime or threat of death or serious bodily harm to any person, or

(3) Anomalies that reveal a potential vulnerability to U.S. communications security. Communications for which the Attorney General or DIRNSA/CHCSS's waiver is sought should be forwarded to NSA/CSS, Attn: P02.

5.5. ~~(S-CCO)~~ Radio Communications with a Terminal in the UNITED STATES.

a. All radio communications that pass over channels with a terminal in the UNITED STATES must be processed through a computer scan dictionary or similar device unless those communications occur over channels used exclusively by a FOREIGN POWER.

b. International common-access radio communications that pass over channels with a terminal in the UNITED STATES [redacted] communications, may be processed without the use of a computer scan dictionary or similar device if necessary to determine whether a channel contains communications of FOREIGN INTELLIGENCE interest which NSA may wish to collect. Such processing may not exceed two hours without the specific prior written approval of the DDO and, in any event, shall be limited to the minimum amount of time necessary to determine the nature of communications on the channel and the amount of such communications that include FOREIGN INTELLIGENCE. Once it is determined that the channel contains sufficient communications of FOREIGN INTELLIGENCE interest to

warrant COLLECTION and exploitation to produce FOREIGN INTELLIGENCE, a computer scan dictionary or similar device must be used for additional processing.

c. Copies of all DDO written approvals made pursuant to 5.5.b. must be provided to the General Counsel and the Inspector General.

SECTION 6 – RETENTION

6.1. ~~(S-CCO)~~ Retention of Communications to, from or About U.S. PERSONS.

a. Except as otherwise provided in Annex A, Appendix 1, Section 4, communications to, from or about U.S. PERSONS that are intercepted by the USSS may be retained in their original or transcribed form only as follows:

(1) Unenciphered communications not thought to contain secret meaning may be retained for five years unless the DDO determines in writing that retention for a longer period is required to respond to authorized FOREIGN INTELLIGENCE requirements.

(2) Communications necessary to maintain technical data bases for cryptanalytic or traffic analytic purposes may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future FOREIGN INTELLIGENCE requirement. Sufficient duration may vary with the nature of the exploitation and may consist of any period of time during which the technical data base is subject to, or of use in, cryptanalysis. If a U.S. PERSON'S identity is not necessary to maintaining technical data bases, it should be deleted or replaced by a generic term when practicable.

b. Communications which could be disseminated under Section 7, below (i.e., without elimination of references to U.S. PERSONS) may be retained in their original or transcribed form.

6.2. ~~(S-CCO)~~ Access. Access to raw traffic storage systems which contain identities of U.S. PERSONS must be limited to SIGINT production personnel.

SECTION 7 – DISSEMINATION

7.1. ~~(S-CCO)~~ Focus of SIGINT Reports. All SIGINT reports will be written so as to focus solely on the activities of foreign entities and persons and their agents. Except as provided in Section 7.2., FOREIGN INTELLIGENCE information concerning U.S. PERSONS must be disseminated in a manner which does not identify the U.S. PERSON. Generic or general terms or phrases must be substituted for the identity (e.g., "U.S. firm" for the specific name of a U.S. CORPORATION or "U.S. PERSON" for the specific name of a U.S. PERSON). Files containing the identities of U.S. persons deleted from SIGINT reports will be maintained for a maximum period of one year and any requests from SIGINT customers for such identities should be referred to P02.

7.2. ~~(S-CCO)~~ Dissemination of U.S. PERSON Identities. SIGINT reports may include the identification of a U.S. PERSON only if one of the following conditions is met and a determination is made

by the appropriate approval authority that the recipient has a need for the identity for the performance of his official duties:

a. The U.S. PERSON has CONSENTED to the dissemination of communications of, or about, him or her and has executed the CONSENT form found in Annex H of this USSID, or

b. The information is PUBLICLY AVAILABLE (i.e., the information is derived from unclassified information available to the general public), or

c. The identity of the U.S. PERSON is necessary to understand the FOREIGN INTELLIGENCE information or assess its importance. The following nonexclusive list contains examples of the type of information that meet this standard:

(1) FOREIGN POWER or AGENT OF A FOREIGN POWER. The information indicates that the U.S. PERSON is a FOREIGN POWER or an AGENT OF A FOREIGN POWER.

(2) Unauthorized Disclosure of Classified Information. The information indicates that the U.S. PERSON may be engaged in the unauthorized disclosure of classified information.

(3) International Narcotics Activity. The information indicates that the individual may be engaged in international narcotics trafficking activities. (See Annex J of this USSID for further information concerning individuals involved in international narcotics trafficking).

(4) Criminal Activity. The information is evidence that the individual may be involved in a crime that has been, is being, or is about to be committed, provided that the dissemination is for law enforcement purposes.

(5) Intelligence TARGET. The information indicates that the U.S. PERSON may be the TARGET of hostile intelligence activities of a FOREIGN POWER.

(6) Threat to Safety. The information indicates that the identity of the U.S. PERSON is pertinent to a possible threat to the safety of any person or organization, including those who are TARGETS, victims or hostages of INTERNATIONAL TERRORIST organizations. Reporting units shall identify to P02 any report containing the identity of a U.S. PERSON reported under this subsection (6). Field reporting to P02 should be in the form of a CRITICOMM message (DDI XAO) and include the report date-time-group (DTG), product serial number and the reason for inclusion of the U.S. PERSON'S identity.

(7) Senior Executive Branch Officials. The identity is that of a senior official of the Executive Branch of the U.S. Government. In this case only the official's title will be disseminated. Domestic political or personal information on such individuals will be neither disseminated nor retained.

7.3. ~~(S-CCO)~~ Approval Authorities. Approval authorities for the release of identities of U.S. persons under Section 7 are as follows:

a. DIRNSA/CHCSS. DIRNSA/CHCSS must approve dissemination of:

(1) The identities of any senator, congressman, officer, or employee of the Legislative Branch of the U.S. Government.

(2) The identity of any person for law enforcement purposes.

b. Field Units and NSA Headquarters Elements. All SIGINT production organizations are authorized to disseminate the identities of U.S. PERSONS when:

(1) The identity is pertinent to the safety of any person or organization.

(2) The identity is that of a senior official of the Executive Branch.

(3) The U.S. PERSON has CONSENTED under paragraph 7.2.a. above.

c. DDO and Designees.

(1) In all other cases, U.S. PERSON identities may be released only with the prior approval of the Deputy Director for Operations, the Assistant Deputy Director for Operations, the Chief, P02, the Deputy Chief, P02, or, in their absence, the Senior Operations Officer of the National SIGINT Operations Center. The DDO or ADDO shall review all U.S. identities released by these designees as soon as practicable after the release is made.

(1) For law enforcement purposes involving narcotics related information, DIRNSA has granted to the DDO authority to disseminate U.S. identities. This authority may not be further delegated.

7.4. (U) Privileged Communications and Criminal Activity. All proposed disseminations of information constituting U.S. PERSON privileged communications (e.g., attorney/client, doctor/patient) and all information concerning criminal activities or criminal or judicial proceedings in the UNITED STATES must be reviewed by the Office of General Counsel prior to dissemination.

7.5. (U) Improper Dissemination. If the name of a U.S. PERSON is improperly disseminated, the incident should be reported to P02 within 24 hours of discovery of the error.

SECTION 8 – RESPONSIBILITIES

8.1. (U) Inspector General.
The Inspector General shall:

a. Conduct regular inspections and perform general oversight of NSA/CSS activities to ensure compliance with this USSID.

b. Establish procedures for reporting by Key Component and Field Chiefs of their activities and practices for oversight purposes.

c. Report to the DIRNSA/CHCSS, annually by 31 October, concerning NSA/CSS compliance with this USSID.

d. Report quarterly with the DIRNSA/CHCSS and General Counsel to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense (Intelligence Oversight).

8.2. (U) General Counsel. The General Counsel shall:

a. Provide legal advice and assistance to all elements of the USSS regarding SIGINT activities. Requests for legal advice on any aspect of these procedures should be sent by CRITICOMM to DDI XDI, or by NSA/CSS secure telephone 963-3121, or [redacted]

b. Prepare and process all applications for Foreign Intelligence Surveillance Court orders and requests for Attorney General approvals required by these procedures.

c. Advise the Inspector General in inspections and oversight of USSS activities.

d. Review and assess for legal implications as requested by the DIRNSA/CHCSS, Deputy Director, Inspector General or Key Components Chief, all new major requirements and internally generated USSS activities.

e. Advise USSS personnel of new legislation and case law that may affect USSS missions, functions, operations, activities, or practices.

f. Report as required to the Attorney General and the President's Intelligence Oversight Board and provide copies of such reports to the DIRNSA/CHCSS and affected agency elements.

g. Process requests from any DoD intelligence component for authority to use signals as described in Procedure 5, Part 5, of DoD 5240.1-R, for periods in excess of 90 days in the development, test, or calibration of ELECTRONIC SURVEILLANCE equipment and other equipment that can intercept communications.

8.3. (U) Deputy Director for Operations (DDO).
The DDO shall:

a. Ensure that all SIGINT production personnel understand and maintain a high degree of awareness and sensitivity to the requirements of this USSID.

b. Apply the provisions of this USSID to all SIGINT production activities. The DDO staff focal point for USSID 18 matters is P02 (use CRITICOMM DDI XAO).

c. Conduct necessary reviews of SIGINT production activities and practices to ensure consistency with this USSID.

d. Ensure that all new major requirements levied on the USSS or internally generated activities are considered for review by the General Counsel. All activities that raise questions of law or the proper interpretation of this USSID must be reviewed by the General Counsel prior to acceptance or execution.

8.4. (U) All Elements of the USSS. All elements of the USSS shall:

a. Implement this directive upon receipt.

b. Prepare new procedures or amend or supplement existing procedures as required to ensure adherence to this USSID. A copy of such procedures shall be forwarded to NSA/CSS, Attn: P02.

c. Immediately inform the DDO of any tasking or instructions that appear to require actions at variance with this USSID.

d. Promptly report to the NSA Inspector General and consult with the NSA General Counsel on all activities that may raise a question of compliance with this USSID.

SECTION 9 – DEFINITIONS

9.1. ~~(S-CCO)~~ AGENT OF A FOREIGN POWER means:

a. Any person, other than a U.S. PERSON, who:

(1) Acts in the UNITED STATES as an officer or employee of a FOREIGN POWER, or as a member of a group engaged in INTERNATIONAL TERRORISM or activities in preparation therefor; or

(2) Acts for, or on behalf of, a FOREIGN POWER that engages in clandestine intelligence activities in the UNITED STATES contrary to the interests of the UNITED STATES, when the circumstances of such person's presence in the UNITED STATES indicate that such person may engage in such activities in the UNITED STATES, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

b. Any person, including a U.S. PERSON, who:

(1) Knowingly engages in clandestine intelligence gathering activities for, or on behalf of, a FOREIGN POWER, which activities involve, or may involve, a violation of the criminal statutes of the UNITED STATES; or

(2) Pursuant to the direction of an intelligence service or network of a FOREIGN POWER, knowingly engages in any other clandestine intelligence activities for, or on behalf of, such FOREIGN POWER, which activities involve or are about to involve, a violation of the criminal statutes of the UNITED STATES; or

(3) Knowingly engages in sabotage or INTERNATIONAL TERRORISM, or activities that are in preparation therefor, for or on behalf of a FOREIGN POWER; or

(4) Knowingly aids or abets any person in the conduct of activities described in paragraphs 9.1.b.(1) through (3) or knowingly conspires with any person to engage in those activities.

c. For all purposes other than the conduct of ELECTRONIC SURVEILLANCE as defined by the Foreign Intelligence Surveillance Act (see Annex A), the phrase "AGENT OF A FOREIGN POWER" also means any person, including U.S. PERSONS outside the UNITED STATES, who are officers or employees of a FOREIGN POWER, or who act unlawfully for or pursuant to the direction of a FOREIGN POWER, or who are in contact with or acting in collaboration with an intelligence or security service of a FOREIGN POWER for the purpose of providing access to information or material classified by the UNITED STATES Government and to which the person has or has had access. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this provision,

absent evidence that the person is taking direction from or acting in knowing concert with a FOREIGN POWER.

9.2. ~~(S)~~ COLLECTION means intentional tasking or SELECTION of identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record.

9.3. (U) COMMUNICANT means a sender or intended recipient of a communication.

9.4. (U) COMMUNICATIONS ABOUT A U.S. PERSON are those in which the U.S. PERSON is identified in the communication. A U.S. PERSON is identified when the person's name, unique title, address, or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A mere reference to a product by brand name or manufacturer's name, e.g., "Boeing 707" is not an identification of a U.S. person.

9.5. (U) CONSENT, for SIGINT purposes, means an agreement by a person or organization to permit the USSS to take particular actions that affect the person or organization. An agreement by an organization with the National Security Agency to permit COLLECTION of information shall be deemed valid CONSENT if given on behalf of such organization by an official or governing body determined by the General Counsel, National Security Agency, to have actual or apparent authority to make such an agreement.

9.6. (U) CORPORATIONS, for purposes of this USSID, are entities legally recognized as separate from the persons who formed, own, or run them. CORPORATIONS have the nationality of the nation state under whose laws they were formed. Thus, CORPORATIONS incorporated under UNITED STATES federal or state law are U.S. PERSONS.

9.7. (U) ELECTRONIC SURVEILLANCE means:

a. In the case of an electronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is a party to the communication.

b. In the case of a nonelectronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is visibly present at the place of communication.

c. The term ELECTRONIC SURVEILLANCE does not include the use of radio direction finding equipment solely to determine the location of a transmitter.

9.8. ~~(S)~~ FOREIGN COMMUNICATION means a communication that has at least one COMMUNICANT outside of the UNITED STATES, or that is entirely among FOREIGN POWERS or between a FOREIGN POWER and officials of a FOREIGN POWER, but does not include communications intercepted by ELECTRONIC SURVEILLANCE directed at premises in the UNITED STATES used predominantly for residential purposes.

9.9. (U) FOREIGN INTELLIGENCE means information relating to the capabilities, intentions, and activities of FOREIGN POWERS, organizations, or persons, and for purposes of this USSID includes both positive FOREIGN INTELLIGENCE and counterintelligence.

9.10. (U) FOREIGN POWER means:

a. A foreign government or any component thereof, whether or not recognized by the UNITED STATES,

b. A faction of a foreign nation or nations, not substantially composed of UNITED STATES PERSONS,

c. An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments,

d. A group engaged in INTERNATIONAL TERRORISM or activities in preparation therefor,

e. A foreign-based political organization, not substantially composed of UNITED STATES PERSONS, or

f. An entity that is directed and controlled by a foreign government or governments.

9.11. (U) INTERCEPTION means the acquisition by the USSS through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form, but does not include the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signal.

9.12. (U) INTERNATIONAL TERRORISM means activities that:

a. Involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the UNITED STATES or of any State, or that would be a criminal violation if committed within the jurisdiction of the UNITED STATES or any State, and

b. Appear to be intended:

(1) to intimidate or coerce a civilian population,

(2) to influence the policy of a government by intimidation or coercion, or

(3) to affect the conduct of a government by assassination or kidnapping, and

c. Occur totally outside the UNITED STATES, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

9.13. (U) PUBLICLY AVAILABLE INFORMATION means information that has been published or broadcast for general public consumption, is available on request to a member of the general public, has been seen or heard by a casual observer, or is made available at a meeting open to the general public.

9.14. ~~(C)~~ SELECTION, as applied to manual and electronic processing activities, means the intentional insertion of a [redacted] telephone number, [redacted] into a computer scan dictionary or manual scan guide for the purpose of identifying messages of interest and isolating them for further processing.

9.15. ~~(C)~~ SELECTION TERM means the composite of individual terms used to effect or defeat SELECTION of particular communications for the purpose of INTERCEPTION. It comprises the entire term or series of terms so used, but not any segregable term contained therein. It applies to both electronic and manual processing.

9.16. (U) TARGET, OR TARGETING: See COLLECTION.

9.17. (U) UNITED STATES, when used geographically, includes the 50 states and the District of Columbia, Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, the Northern Mariana Islands, and any other territory or possession over which the UNITED STATES exercises sovereignty.

9.18. ~~(C)~~ UNITED STATES PERSON:

a. A citizen of the UNITED STATES,

b. An alien lawfully admitted for permanent residence in the UNITED STATES,

c. Unincorporated groups and associations a substantial number of the members of which constitute a. or b. above, or

d. CORPORATIONS incorporated in the UNITED STATES, including U.S. flag nongovernmental aircraft or vessels, but not including those entities which are openly acknowledged by a foreign government or governments to be directed and controlled by them.

e. The following guidelines apply in determining whether a person is a U.S. PERSON:

(1) A person known to be currently in the United States will be treated as a U.S. PERSON unless that person is reasonably identified as an alien who has not been admitted for permanent residence or if the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is not a U.S. PERSON.

(2) A person known to be currently outside the UNITED STATES, or whose location is not known, will not be treated as a U.S. PERSON unless such person is reasonably identified as such or the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is a U.S. PERSON.

(3) A person known to be an alien admitted for permanent residence may be assumed to have lost status as a U.S. PERSON if the person leaves the UNITED STATES and it is known that the person is not in compliance with the administrative formalities provided by law (8 U.S.C. Section 1203) that enable such persons to reenter the UNITED STATES without regard to the provisions of law that would otherwise restrict an alien's entry into the UNITED STATES. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

(4) An unincorporated association whose headquarters are located outside the UNITED STATES may be presumed not to be a U.S. PERSON unless the USSS has information indicating that a substantial number of members are citizens of the UNITED STATES or aliens lawfully admitted for permanent residence.

(5) CORPORATIONS have the nationality of the nation-state in which they are incorporated. CORPORATIONS formed under U.S. federal or state law are thus U.S. persons, even if the corporate stock is foreign-owned. The only exception set forth above is CORPORATIONS which are openly acknowledged to be directed and controlled by foreign governments. Conversely, CORPORATIONS incorporated in foreign countries are not U.S. PERSONS even if that CORPORATION is a subsidiary of a U.S. CORPORATION.

(6) Nongovernmental ships and aircraft are legal entities and have the nationality of the country in which they are registered. Ships and aircraft fly the flag and are subject to the law of their place of registration.

~~TOP SECRET//STLW//SI//ORCON/NOFORN~~

No. OP 2008-0009

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

OFFICE OF THE INSPECTOR GENERAL

~~(S//NF)~~ REVIEW OF THE PARTICIPATION OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE IN THE PRESIDENT'S SURVEILLANCE PROGRAM

July 2, 2009

ROSLYN A. MAZER
INSPECTOR GENERAL

Copy No.

CL BY: 2385885
CL
REASON: 1.4(C),(G)
DECL ON: 20340218
DRV FROM: MIS S-06,
ODNI COM T-08

This page intentionally left blank.

(U) TABLE OF CONTENTS

		PAGE
I.	(U) EXECUTIVE SUMMARY	2
II.	(U) INTRODUCTION	3
III.	(U) SCOPE AND METHODOLOGY	3
IV.	(U) DISCUSSION OF FINDINGS	4
	A. (U) Initial Response by the President and Congress to the Terrorist Attacks of September 11, 2001 (U)	4
	B. ~~(TS//STLW//SI//OC/NF)~~ ODNI Role in Preparing Threat Assessments in Support of the Program	6
	C. ~~(TS//STLW//SI//OC//NF)~~ NCTC Use of the Program to Support Counterterrorism Analysis	10
	D. [redacted]	12
	E. ~~(TS//STLW//SI//OC/NF)~~ NCTC Role in Identifying Program Targets or Tasking Collection	13
	F. ~~(S/NF)~~ ODNI Oversight of the Program	13
V.	(U) CONCLUSION	16
VI.	(U) APPENDIX – STRUCTURE OF THE ODNI - 2005	17

This page intentionally left blank.

~~(S/NF)~~ REVIEW OF THE PARTICIPATION OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE IN THE PRESIDENT'S SURVEILLANCE PROGRAM

I. (U) EXECUTIVE SUMMARY

~~(TS//STLW//SI//OC/NF)~~ The Office of Inspector General (OIG), Office of the Director of National Intelligence (ODNI), was one of five Intelligence Community Inspectors General that conducted a review of their agency's participation in the President's Surveillance Program (hereafter "the Program"), a top secret National Security Agency (NSA) electronic surveillance activity undertaken at the direction of the President. The Program became operational on October 4, 2001, three weeks after the deadly terrorist attacks of September 11, 2001. The review examined the ODNI's involvement in the Program from the period beginning with the stand-up of the ODNI in April 2005 through the termination of the Program in January 2007.

~~(TS//STLW//SI//OC/NF)~~ The ODNI's primary role in the Program was the preparation of the threat assessments that summarized the al Qaeda terrorist threat to the United States and were used to support the periodic reauthorization of the Program. That role began in April 2005, shortly after the ODNI stand-up and contemporaneous with the arrival of General Michael Hayden as the first Principal Deputy Director of National Intelligence (PDDNI). Prior to his ODNI appointment, Hayden was Director of NSA. In April 2005, ODNI personnel in the National Counterterrorism Center (NCTC) began to prepare the first of 12 Program threat assessments. In coordination with the Department of Justice (DOJ), then Director of National Intelligence (DNI) John Negroponte or PDDNI Hayden approved 12 ODNI-prepared threat assessments over an 18-month period. Once approved by the DNI or PDDNI, the Program threat assessments were reviewed and approved by the Secretary of Defense, and were subsequently used by DOJ, NSA, and White House personnel in support of the Program reauthorization. In addition to the preparation of the threat assessments, we found that NCTC used Program information in producing analytical products that were distributed to senior IC community officials and analysts. [redacted]

~~(TS//STLW//SI//OC/NF)~~ During the review, we made several related findings and observations. We learned that the ODNI usage of Program-derived information in ODNI intelligence products was consistent with the standard rules and procedures for handling NSA intelligence. We learned that ODNI personnel were not involved in nominating specific targets for collection through the Program. While ODNI personnel were identified as having contact [redacted] regarding the Program, we found that those communications were limited in frequency and scope. We also found that the ODNI intelligence oversight components -- the Civil Liberties Protection Officer (CLPO), Office of General Counsel (OGC), and the OIG -- had little involvement in oversight of the Program and had limited opportunity to participate in Program oversight due to delays in ODNI oversight personnel being granted access to the

Program and temporary resource limitations attendant to the stand-up of the ODNI. Finally, we found that the 2008 amendments to Executive Order 12333 and the current ODNI staffing levels provide the ODNI oversight components with sufficient resources and authority to fulfill their current oversight responsibilities, assuming timely notification.

II. (U) INTRODUCTION

~~(TS//STLW//SI//OC/NF)~~ *The Foreign Intelligence Surveillance Act Amendments Act of 2008*, Pub L. No. 110-261, 122 Stat. 2438 (hereafter "FISA Amendments Act") required the IGs of the DOJ, ODNI, NSA, Department of Defenses (DOD), and any other element of the intelligence community that participated in the President's Surveillance Program to conduct a comprehensive review of the Program.[1] The FISA Amendments Act defined the "President's Surveillance Program" as the "intelligence activity involving communications authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005." In response to this tasking, the IGs of the following five agencies were identified as having a role in Program review: DOJ, ODNI, NSA, DOD, and the Central Intelligence Agency (CIA).

~~(S//NF)~~ The participating IGs organized the review in a manner where each OIG conducted a review of its own agency's involvement in the Program. CIA IG John Helgerson was initially designated by the IGs to coordinate the review and oversee the preparation of an interim report due within 60 days after the enactment of the Act, and a later final report due not later than 1 year after the enactment of the Act.[2] Because of IG Helgerson's recent retirement, DOJ IG Glenn Fine was selected to coordinate the preparation of the final report. This report contains the results of the ODNI OIG review.

III. (U) SCOPE AND METHODOLOGY

~~(TS//STLW//SI//OC/NF)~~ We sought to identify the role of the ODNI in implementing the Program beginning with the stand-up of the ODNI in April 2005 through the Program's termination in January 2007. This review examined the:

A. Role of the ODNI and its component the National Counterterrorism Center (NCTC) in drafting and coordinating the threat assessments that supported the periodic reauthorization of the Program;

---

[1] ~~(S//NF)~~ The Program is also known within the Intelligence Community by the cover term STELLARWIND. The Program is a Top Secret/Sensitive Compartmented Information (SCI) program.

[2] (U) The participating IGs submitted an interim report, dated September 10, 2008, to the Chairman and Ranking member of the Senate Select Committee on Intelligence (SSCI) and a revised interim report, dated November 24, 2008, to the Chairman and Ranking member of the House of Representatives Permanent Select Committee on Intelligence (HPSCI).

B. NCTC's use of Program information to support counterterrorism analysis;

C. NCTC's role in identifying Program targets and tasking Program collection;

D. [redacted] and

F. Role of the ODNI in providing compliance oversight of the Program.

~~(TS//STLW//SI//OC/NF)~~ During the review, we interviewed 23 current or former ODNI officials and employees involved in the Program. The ODNI personnel we interviewed were cooperative and helpful. Our interviews included the following ODNI senior officials:

John Negroponte, former Director of National Intelligence
Michael McConnell, former Director of National Intelligence
Michael V. Hayden, former Principal Deputy Director of National Intelligence
Ronald Burgess, former Acting Principal Deputy Director of National Intelligence
David R. Shedd, Deputy Director of National Intelligence for Policy, Plans, and Requirements
Alexander W. Joel, Civil Liberties Protection Officer
Edward Maguire, former Inspector General
Benjamin Powell, former General Counsel
Corin Stone, Deputy General Counsel and Acting General Counsel
Joel Brenner, former National Counterintelligence Executive[3]
John Scott Redd, former NCTC Director
Michael Leiter, NCTC Director

~~(S//NF)~~ In addition to the interviews noted above, we reviewed Program-related documents made available by the NSA OIG, the DOJ OIG, and the ODNI OGC.

IV. (U) DISCUSSION OF FINDINGS

~~(TS//STLW//SI//OC/NF)~~ The following discussion contains our findings regarding the topics identified above. First, we briefly describe the terrorist attacks of September 11, 2001, and the initial government response to the attacks, including the authorization of the President's Surveillance Program. Next, we discuss the ODNI and NCTC role in implementing the Program. Finally, we set forth our conclusions and observations.

A. (U) Initial Response by the President and Congress to the Terrorist Attacks of September 11, 2001

(U) The devastating al Qaeda terrorist attacks against the United States quickly triggered an unprecedented military and intelligence community response to protect the

[3] (U) Brenner was the NSA Inspector General before joining the ODNI.

country from additional attacks. The following quote describes the initial terrorist attacks and the intended al Qaeda goal to deliver a decapitating strike against our political institutions.

> (U) On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial airliners, each carefully selected to be fully loaded with jet fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners were targeted at the Nation's financial center in New York and were deliberately flown into the Twin Towers of the World Trade Center. The third was targeted at the headquarters of the Nation's Armed Forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was evidently the White House or the Capitol, strongly suggesting that its intended mission was to strike a decapitation blow on the Government of the United States – to kill the President, the Vice President, or Members of Congress. The attacks of September 11th resulted in approximately 3,000 deaths – the highest single-day death toll from hostile foreign attacks in the Nation's history.[4]

(U) On September 14, 2001, in response to the attacks, the President issued a *Declaration of National Emergency by Reason of Certain Terrorist Attacks* stating that "(a) national emergency exists by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and continuing immediate threat of further attacks on the United States."[5]

(U) On September 18, 2001, by an overwhelming majority in both the Senate and House of Representatives, a joint resolution was passed that authorized the use of United States military force against those responsible for the terrorist attacks launched against the United States. The joint resolution, also known as the *Authorization for Use of Military Force (AUMF)*, is often cited by White House and DOJ officials as one of the principal legal authorities upon which the Program is based. In relevant part, the AUMF provides:[6]

> (a) IN GENERAL – That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organization or persons, in order to

---

[4] (U) This summary of the events of September 11, 2001, was prepared by DOJ personnel and is set forth in the unclassified DOJ "White Paper" entitled *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, dated January 19, 2006.

[5] (U) Proclamation 7463, 66 Fed. Reg. No. 181, September 14, 2001.

[6] (U) *Authorization for Use of Military Force*, Section 2(a), Pub. L. No. 170-40, 115 Stat. 224, September 18, 2001.

prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

~~(TS//STLW//SI//OC/NF)~~ On October 4, 2001, three days before the start of overt military action against the al Qaeda and Taliban terrorist camps, the President authorized the Secretary of Defense to implement the President's Surveillance Program.[7] The Program, a closely held top-secret NSA electronic surveillance project, authorized the Secretary of Defense to employ within the United States the capabilities of the DOD, including but not limited to the signals intelligence capabilities of the NSA, to collect international terrorism-related foreign intelligence information under certain specified circumstances. Each Program reauthorization was supported by a written threat assessment, approved by a senior Intelligence Community official, that described the threat of a terrorist attack against the United States.

(U) On October 7, 2001, in a national television broadcast, the President announced the start of military operations against al Qaeda and Taliban terrorist camps in Afghanistan.[8]

~~(TS//STLW//SI//OC/NF)~~ On April 22, 2005, the ODNI began operations as the newest member of the Intelligence Community. The ODNI was created, in part, in response to the findings of the *Independent National Commission on Terrorist Attacks Upon the United States* (hereafter 9/11 Commission) that recommended the creation of a national "Director of National Intelligence" to oversee and coordinate the planning, policy, and budgets of the Intelligence Community.[9] In late April 2005, ODNI personnel began to prepare the threat assessments used in the periodic reauthorization of the Program. In June 2005, ODNI officials began to approve the threat assessments.

B. ~~(TS//STLW//SI//OC/NF)~~ ODNI Role in Preparing Threat Assessments in Support of the Program Reauthorizations

~~(TS//STLW//SI//OC/NF)~~ Prior to the ODNI's involvement in the Program, the Program was periodically reauthorized approximately every 30 to 45 days pursuant to a reauthorization process overseen by DOJ, NSA, and White House personnel. Each reauthorization relied, in part, on a written threat assessment approved by a senior Intelligence Community official that described the current threat of a terrorist attack against the United States and contained the approving official's recommendation regarding the need to reauthorize the Program. Before the ODNI's involvement in the

---

[7] ~~(TS//STLW//SI//OC/NF)~~ The NSA materials we reviewed identified October 4, 2001, as the date of the first Program authorization.

[8] (U) The CNN.com webpage article entitled *President announces opening of attack*, dated, October 7, 2001, provides a summary of the President's announcement and describes the national television broadcast.

[9] (U) While the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) that created the ODNI was signed by the President on December 17, 2004, the actual ODNI stand-up occurred months later. The official ODNI history, *A Brief History of the ODNI's Founding*, sets April 22, 2005, as the date when the ODNI commenced operations.

Program, every threat assessment prepared by the Intelligence Community in support of the Program reauthorization identified the threat of a terrorist attack against the United States and recommended that the Program be reauthorized. Accordingly, the Program was regularly reauthorized during the approximately 3-year period prior to the involvement of the ODNI. During that period, the Director of Central Intelligence or his designee approved 31 threat assessments in support of the reauthorization of the Program.

~~(TS//STLW//SI//OC/NF)~~ In reviewing the circumstances that led to the decision to transfer responsibility for preparing the Program threat assessments to the ODNI, we found that the ODNI does not have identifiable records regarding that decision. Senior ODNI officials involved with the Program told us that after the merger of the Terrorist Threat Integration Center (TTIC) into the NCTC, and the later incorporation of NCTC into the ODNI, it made sense for the ODNI to take responsibility for preparing the Program threat assessments as both TTIC and NCTC previously handled that task. Former PDDNI Hayden told us that the primary reason that the ODNI become involved in the Program was the statutory creation of the new DNI position as the senior Intelligence Community advisor to the President. When Ambassador Negroponte was confirmed as the first DNI, Hayden and other senior intelligence officials believed that DNI Negroponte, as the President's new senior intelligence advisor, should make the Intelligence Community's recommendation to the President regarding the need to renew the Program. Hayden commented that the new DNI's involvement in this important intelligence program enhanced the DNI's role as the leader of the Intelligence Community and gave immediate credibility to the ODNI as a new intelligence agency.

~~(TS//STLW//SI//OC/NF)~~ Once the ODNI became involved in the Program, the preparation and approval of the threat assessments became the ODNI's primary Program role.[10] Beginning in April 2005, and continuing at about 30 to 45 day intervals until the Program's termination in January 2007, ODNI personnel prepared and approved 12 written threat assessments in support of the periodic reauthorization of the Program. We found that the ODNI threat assessments were drafted by experienced NCTC personnel who prepared the documents following an established DOJ format used in earlier Program reauthorizations. NCTC analysts prepared the threat assessments in a memorandum format, usually 12 to 14 pages in length. Senior ODNI and NCTC officials told us that each threat assessment was intended to set forth the ODNI's view regarding the current threat of an al Qaeda attack against the United States and to provide the DNI's recommendation whether to continue the Program. NCTC personnel involved in preparing the threat assessments told us that the danger of a terrorist attack described in the threat assessments was sobering and "scary," resulting in the threat assessments becoming known by ODNI and Intelligence Community personnel involved in the Program as the "scary memos."

---

[10] ~~(TS//STLW//SI//OC/NF)~~ The joint interim report prepared by the participating IGs notified congressional oversight committees that the review would examine the ODNI's involvement in preparing "threat assessments and legal certifications" submitted in support of the Program. Because we did not identify any ODNI officials executing a legal certification, we treated our review of the legal certifications to be the same as the review of the threat assessments. The Attorney General made legal certifications in support of the Program that are addressed in the DOJ OIG report.

~~(TS//STLW//SI//OC/NF)~~ During interviews, ODNI personnel said they were aware that the threat assessments were relied upon by DOJ and the White House as the basis for continuing the Program and further understood that if a threat assessment identified a threat against the United States, the Program was likely to be reauthorized. NCTC analysts also said that on a less frequent basis they prepared a related document that set forth a list of al Qaeda-affiliated groups that they understood were targets of the Program. Both the threat assessments and the less frequent list of al Qaeda-affiliated groups underwent the same ODNI approval process.

~~(TS//STLW//SI//OC/NF)~~ We examined the ODNI process for preparing the Program documents, particularly the threat assessments, and found that the documents were drafted by experienced NCTC analysts under the supervision of the NCTC Director and his management staff, who were ultimately responsible for the accuracy of the information in the documents. We determined that the ODNI threat assessments were prepared using evaluated intelligence information chosen from a wide-variety of Intelligence Community sources. ODNI personnel told us that during the period when the ODNI prepared the threat assessments, the Intelligence Community had access to fully evaluated intelligence that readily supported the ODNI assessments that al Qaeda terrorists remained a significant threat to the United States.

~~(TS//STLW//SI//OC/NF)~~ Once the ODNI threat assessments were approved within NCTC and by the NCTC Director, the documents were forwarded through an established approval chain to senior ODNI personnel who independently satisfied themselves that the documents were accurate, properly prepared, and in the appropriate format. Throughout the ODNI preparation and approval process, the threat assessments were also subject to varying degrees of review and comment by DOJ and OGC attorneys, including then General Counsel Benjamin Powell and Deputy General Counsel Corin Stone. Powell said his review of the threat assessments was not a legal review, but was focused on spotting issues that might merit further review or analysis. Powell said he relied on DOJ to conduct the legal review. Once the draft threat assessments were subjected to this systematic and multi-layered management and legal review, the documents were provided to the DNI or PDDNI for consideration and, if appropriate, approval. Overall, we found the process used by the ODNI to prepare and obtain approval of the threat assessments was straightforward, reasonable, and consistent with the preparation of other documents requiring DNI or PDDNI approval.

~~(TS//STLW//SI//OC/NF)~~ Negroponte told us that because of time-sensitive issues present in 2005 relating to the ongoing ODNI start-up as a new agency and other Intelligence Community matters requiring his attention, he tasked his deputy, then PDDNI Hayden, to oversee the ODNI approval of the threat assessments and related documents. Negroponte told us that when making this decision, he was aware of Hayden's prior experience with the Program during Hayden's earlier assignment as Director of NSA. In June 2005, shortly after his arrival at ODNI, Hayden received and approved the first ODNI threat assessment. Hayden later approved the next six ODNI threat assessments. After Hayden left the ODNI in May 2006 to become Director of CIA, Negroponte approved the next five ODNI threat assessments, including a December

2006 threat assessment used in the final reauthorization of the Program. In total, Negroponte and Hayden approved 12 ODNI threat assessments prepared in support of the Program reauthorizations.[11]

~~(TS//STLW//SI//OC/NF)~~ In discussing the ODNI process used to prepare and approve the threat assessments, Negroponte told us he was "extremely satisfied" with the quality and content of the threat assessments provided for his approval. He did not recall any inaccuracies or problems relating to preparation of the ODNI threat assessments. Negroponte said the al Qaeda threat information described in the Program threat assessments was consistent with the terrorism threat information found in *The President's Daily Briefing* and other senior-level Intelligence Community products he had read. Hayden had a similar view. Negroponte and Hayden separately told us that when they approved the threat assessments, credible intelligence was readily available to the Intelligence Community that demonstrated the ongoing and dangerous al Qaeda terrorist threat to the United States. Similarly, Negroponte and Hayden each told us that the nature and scope of the al Qaeda terrorist threat to the United States was well documented and easily supported the ODNI threat assessments used in the Program reauthorizations.

~~(TS//STLW//SI//OC/NF)~~ Because of questions raised in the media about the legal basis for the Program, we asked the ODNI personnel involved in the preparation or approval of the threat assessments about their concerns, if any, regarding the legal basis for the Program. We found that ODNI personnel involved in the Program generally understood that the Program had been in operation for several years and was approved by senior Intelligence Community and DOJ officials. During our interviews, ODNI officials told us they were satisfied with the legal basis for the Program, primarily because of their knowledge that the Attorney General and senior DOJ attorneys had personally approved the Program and remained directly involved in the Program reauthorization process. We did not identify any ODNI personnel who believed that the program was unlawful.

~~(TS//STLW//SI//OC/NF)~~ Former ODNI General Counsel Powell told us that after his Program briefings in early 2006, he had questions regarding the DOJ description of the legal authority for the Program but lacked the time to conduct his own legal review of the issue given the many time-sensitive ODNI legal issues that required his attention. Powell said he understood the rationale of DOJ's legal opinion that the Program was lawful and described the DOJ opinion as a "deeply complex issue" with "legal scholarship on both sides." Powell said he recognized that he was a latecomer to a complex legal issue that was previously and continuously approved by DOJ, personally supported by the Attorney General, and was being transitioned to judicial oversight – an idea he strongly supported. Powell said he relied on the DOJ legal opinion regarding the Program and directed his efforts to supporting the Program's transition to judicial oversight under traditional FISA, the 2007 Protect America Act, and the subsequent FISA Amendments Act of 2008.

[11] ~~(TS//STLW//SI//OC/NF)~~ The DNI and PDDNI together approved 12 of the 43 threat assessments used in support of the Program reauthorizations. CIA officials approved the other 31 threat assessments.

~~(TS//STLW//SI//OC/NF)~~ Negroponte recalled having regular contact with senior NSA and DOJ officials who raised no legal concerns to him about the Program. He said he remembered attending a Program-related meeting that included members of the FISA Court who did not raise any legal concerns to him about the authority for the Program and seemed generally supportive of the Program. Negroponte also recalled attending meetings in which the Program was briefed to congressional leadership who not did raise legal concerns to him. Overall, the direct involvement of DOJ and other senior Intelligence Community officials in the Program resulted in Negroponte and other ODNI personnel having few, if any, concerns about the legal basis for the Program.

C. ~~(TS//STLW//SI//OC/NF)~~ NCTC Use of Program Information to Support Counterterrorism Analysis

~~(TS//STLW//SI//OC/NF)~~ The Program information was closely held within the ODNI and was made available to no more than 15 NCTC analysts for review and, if appropriate, use in preparing NCTC analytical products.[12] Generally, the NCTC analysts approved for access received the Program information in the form of finished NSA intelligence products. [redacted] The NCTC analysts said the Program information was subject to stringent security protections [redacted] The NCTC analysts told us they received training regarding proper handling of NSA intelligence. They said they handled the NSA intelligence, including Program information, consistent with the standard rules and procedures for handling NSA intelligence information, including the minimization of U.S. person identities.

~~(TS//STLW//SI//OC/NF)~~ Hayden told us that during his tenure as Director of NSA, he sought to disseminate as much Program information as possible to the Intelligence Community [redacted]

~~(TS//STLW//SI//OC/NF)~~ During our review, NCTC analysts told us they often did not know if the NSA intelligence available to them was derived from the Program. [redacted]

[12] ~~(TS//STLW//SI//OC/NF)~~ The number of NCTC analysts read into the Program ranged from 5 to 15 analysts.

[redacted] On those occasions when the NCTC analysts knew that a particular NSA intelligence product was derived from the Program, the analysts said they reviewed the Program information in the same manner as other NSA intelligence products and, if appropriate, incorporated the Program information into analytical products being prepared for the DNI and other senior intelligence officials. They identified the *President's Terrorism Threat Report* and the *Senior Executive Terrorism Report* as examples of the types of finished intelligence products that would, at times, contain Program information.

~~(TS//STLW//SI//OC/NF)~~ NCTC analysts with Program access said they had broad access to a wide variety of high quality and fully evaluated terrorism related intelligence. In particular, NCTC analysts told us that by virtue of their NCTC assignments, they had access to some of the most sensitive and valuable terrorism intelligence available to the Intelligence Community. NCTC analysts characterized the Program information as being a useful tool, but also noted that the Program information was only one of several valuable sources of information available to them from numerous collection sources and methods. During interviews, NCTC analysts and other ODNI personnel described the Program information as "one tool in the tool box," "one arrow in the quiver," or in other similar phrases to connote that the Program information was not of greater value than other sources of intelligence. The NCTC analysts we interviewed said they could not identify specific examples where the Program information provided what they considered time-sensitive or actionable intelligence, but they generally recalled attending meetings in which the benefits of the Program were discussed. [redacted] The NCTC analysts uniformly told us that during the period when NCTC prepared the threat assessment memoranda, the intelligence demonstrating the al Qaeda threat to the United States was overwhelming and readily available to the Intelligence Community.

~~(TS//STLW//SI//OC/NF)~~ When asked about the value of the Program, Hayden said "without the Program as a skirmish line you wouldn't know what you don't know." He explained that by using the Program to look at a "quadrant of communications" the Intelligence Community was able to assess the threat arising from those communications, which allowed Intelligence Community leaders to make valuable judgments regarding the allocation of national security resources. He said looking at the terrorist threat in this manner was similar to soldiers on a combat patrol who look in all directions for the threat and assign resources based on what they learn. Hayden said that NSA General Counsel Vito Potenza often described the Program as an "early warning system" for terrorist threats, which Hayden thought was an accurate description of the Program. Hayden told us the Program was extremely valuable in protecting the United States from an al Qaeda terrorist attack. Hayden cited [redacted]

[redacted] as examples where the Program information was effectively used to disrupt al Qaeda operatives.[13]

D. [redacted]

[redacted]

[redacted]

[redacted]

E. ~~(TS//STLW//SI//OC/NF)~~ No NCTC Role in Identifying Program Targets and Tasking Collection

~~(TS//STLW//SI//OC/NF)~~ We did not identify any information that indicated that ODNI or NCTC personnel were involved in identifying or nominating targets for collection within the Program. ODNI personnel told us that ODNI and NCTC are non-operational elements of the Intelligence Community and were not involved in nominating targets for Program collection.

F. ~~(S/NF)~~ ODNI Oversight of the Program

~~(TS//STLW//SI//OC/NF)~~ We examined the role of the ODNI oversight components -- CLPO, OIG, and OGC -- in providing compliance oversight for the Program. We found that while the Program was subject to oversight by the NSA OIG, the ODNI oversight components had a limited role in providing oversight for the Program. During the review, we learned that within the first year of the Program, then NSA Director Hayden obtained White House approval allowing the NSA IG and designated NSA OIG officials to be read into the Program to provide compliance oversight for the Program. In furtherance of the NSA oversight program, the NSA IG provided compliance reports and briefings to the NSA Director, NSA General Counsel, and cleared White House personnel, including the Counsel to the President.[16]

~~(TS//STLW//SI//OC/NF)~~ In reviewing the ODNI oversight role regarding the Program, we found that the ODNI oversight components had limited involvement in oversight of the Program. We found that the opportunity for the ODNI to participate in Program oversight was limited by the fact that ODNI oversight personnel were not

[redacted]

[15] ~~(TS//STLW//SI//OC/NF)~~ [redacted]

[16] ~~(S//NF)~~ According to the General Counsel to the President's Intelligence Oversight Board (IOB), the IOB members and staff were not read into the Program and did not receive compliance reports from the NSA IG.

granted timely access to the Program by the White House personnel responsible for approving access. In addition, we found that the newly formed ODNI oversight offices were in varying stages of agency stand-up and lacked the necessary experienced staff and resources to effectively participate in oversight of the Program.

~~(TS//STLW//SI//OC/NF)~~ For example, General Counsel Powell received Program access after his arrival in January 2006, but his predecessor, then Acting General Counsel Corin Stone, was not read into the Program until a few days before Powell in January 2006, several months after the Program became operational within ODNI and only after she had read about the Program in a December 2005 newspaper article.[17] Similarly, CLPO Alexander Joel, who is responsible for reviewing the privacy and civil liberties implications of intelligence activities, requested but did not receive Program access until October 2006, shortly before the Program terminated.[18] Joel told us that Negroponte and Hayden supported his request for Program access, but White House staff delayed approval for several months. Joel said that while waiting for approval of his Program access, Hayden gave him some insight about the Program that did not require the disclosure of compartmented information. Joel found this information helpful in planning his later review. Finally, then ODNI Inspector General Edward Maguire and his oversight staff did not obtain Program access until 2008, long after the Program had terminated.[19]

~~(TS//STLW//SI//OC/NF)~~ Once read into the Program, Powell and Joel were provided with reasonable access to NSA compliance reports and briefings relating to the NSA OIG oversight program. Powell told us that he was satisfied that the NSA IG provided a reasonable degree of Program oversight. Similarly, Joel said he believed that he had received full disclosure regarding the NSA oversight program and found the NSA oversight effort to be reasonable.

~~(TS//STLW//SI//OC/NF)~~ We also learned that the members of the President's Privacy and Civil Liberties Oversight Board (PCLOB) reviewed the Program, in part, in association with Joel.[20] The PCLOB review was contemporaneous with Joel's review

---

[17] (U//~~FOUO~~) Powell was appointed General Counsel in January 2006 and served in that position as a recess appointment until his Senate confirmation in April 2006. Prior to his appointment, Powell was an Associate Counsel to the President and Special Assistant to the President where he worked on initiatives related to the Intelligence Community. However, Powell was not read into the Program while serving at the White House.

[18] (U//~~FOUO~~) Joel is the Civil Liberties Protection Officer (CLPO) with the responsibility for ensuring that the protection of privacy and civil liberties is incorporated in the policies and procedures of the Intelligence Community. The CLPO responsibilities are set forth in the Section 103d of *Intelligence Reform and Terrorism Prevention Act of 2004.*

[19] ~~(S//NF)~~ While OIG personnel were not read into the Program until 2008, OIG officials were alerted to the existence of the NSA collection program through a December 2005 newspaper report. Shortly after that report, the NSA IG told ODNI OIG officials that the NSA OIG was conducting oversight of that NSA program. PDDNI Hayden also told IG Maguire that the NSA program was subject to NSA OIG oversight.

[20] (U) The PCLOB was created by the *Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)*, which requires the Board to "ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism (P.L. 108-458, 2004).

and resulted in an independent and generally favorable finding regarding the NSA implementation of the Program. After the PCLOB review, a PCLOB board member published an editorial article, in part, quoted below, that summarized his observations regarding the NSA effort in implementing the Program.

> There were times, including when the Board was "read into" and given complete access to the operation of the Terrorist Surveillance Program that I wondered whether the individuals doing this difficult job on behalf of all of us were not being too careful, too concerned, about going over the privacy and liberties lines – so concerned, with so many internal checks and balances, that they could miss catching or preventing the bad guys from another attack. And I remember walking out of these briefing sessions in some dark and super-secret agency with the thought: I wish the American people could meet these people and observe what they are doing.[21]

~~(S//NF)~~ In sum, the ODNI oversight components had limited and belated involvement in the oversight of the Program. However, once read into the Program, Powell and Joel determined that the Program was subject to reasonable oversight by the NSA OIG. Moreover, the initial White House delay in granting ODNI oversight personnel access to the Program occurred prior to the 2008 revision to Executive Order (EO) 12333, which expressly grants ODNI oversight components broad access to any information necessary to performing their oversight duties. In particular, EO 12333 provides in relevant part that:

> Section 1.6 *Heads of Elements of the Intelligence Community*. The heads of elements of the Intelligence Community shall:
>
> (h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy and civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their duties.

~~(TS//STLW//SI//OC/NF)~~ EO 12333, as amended, clarifies and strengthens the ODNI's ability to provide compliance oversight. In light of the recent change to EO 12333, and with current staffing, we believe that ODNI's oversight components have sufficient resources and authority to perform their responsibilities to conduct oversight of closely held intelligence activities, assuming timely notification.

---

[21] (U) The quote is taken from a May 5, 2007, article by former PCLOB member Lanny Davis, entitled, "*Why I Resigned From The President's Privacy and Civil Liberties Oversight Board – And Where We Go From Here.*" The article was published on webpage of The Huffington Post, www.huffingtonpost.com.

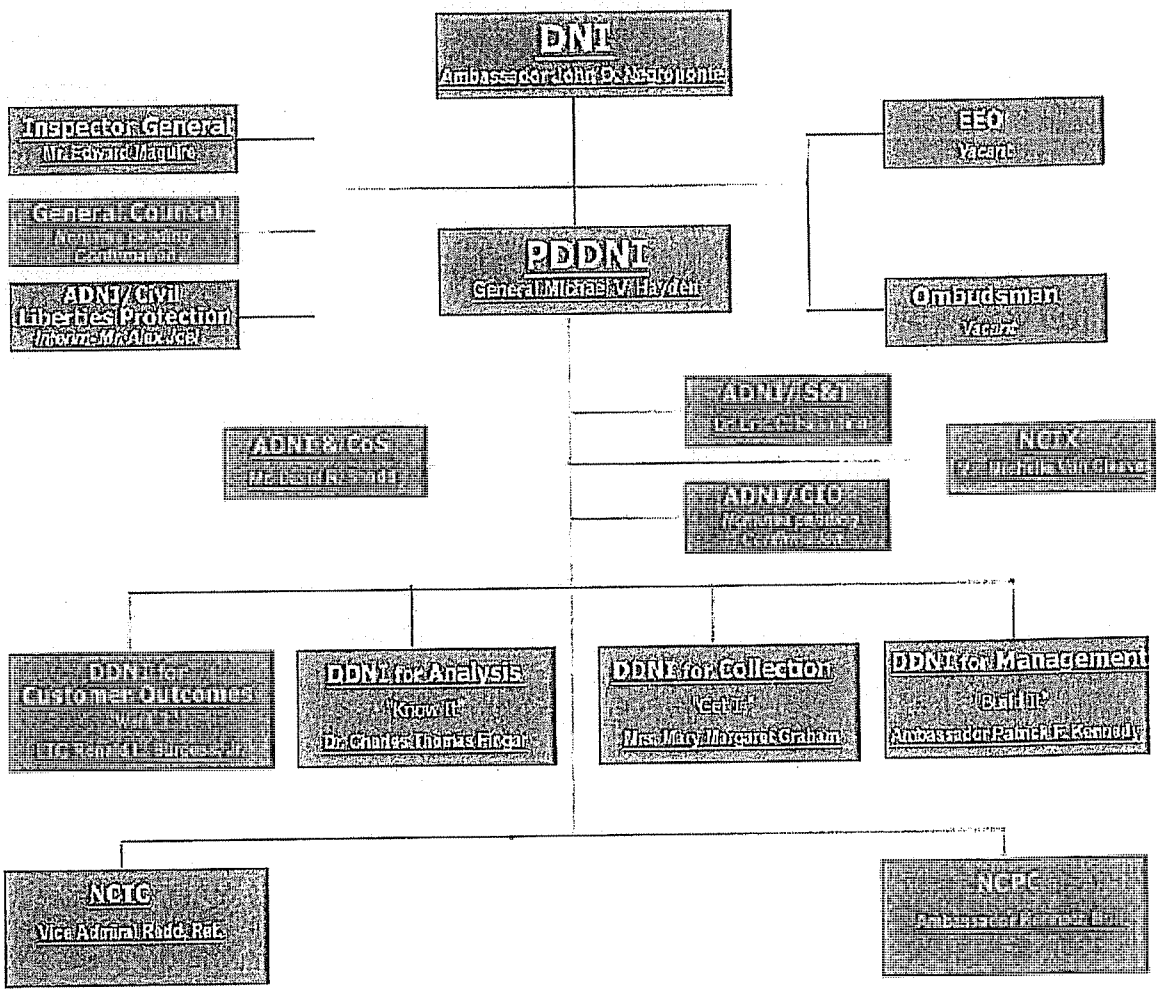
V. (U) CONCLUSION

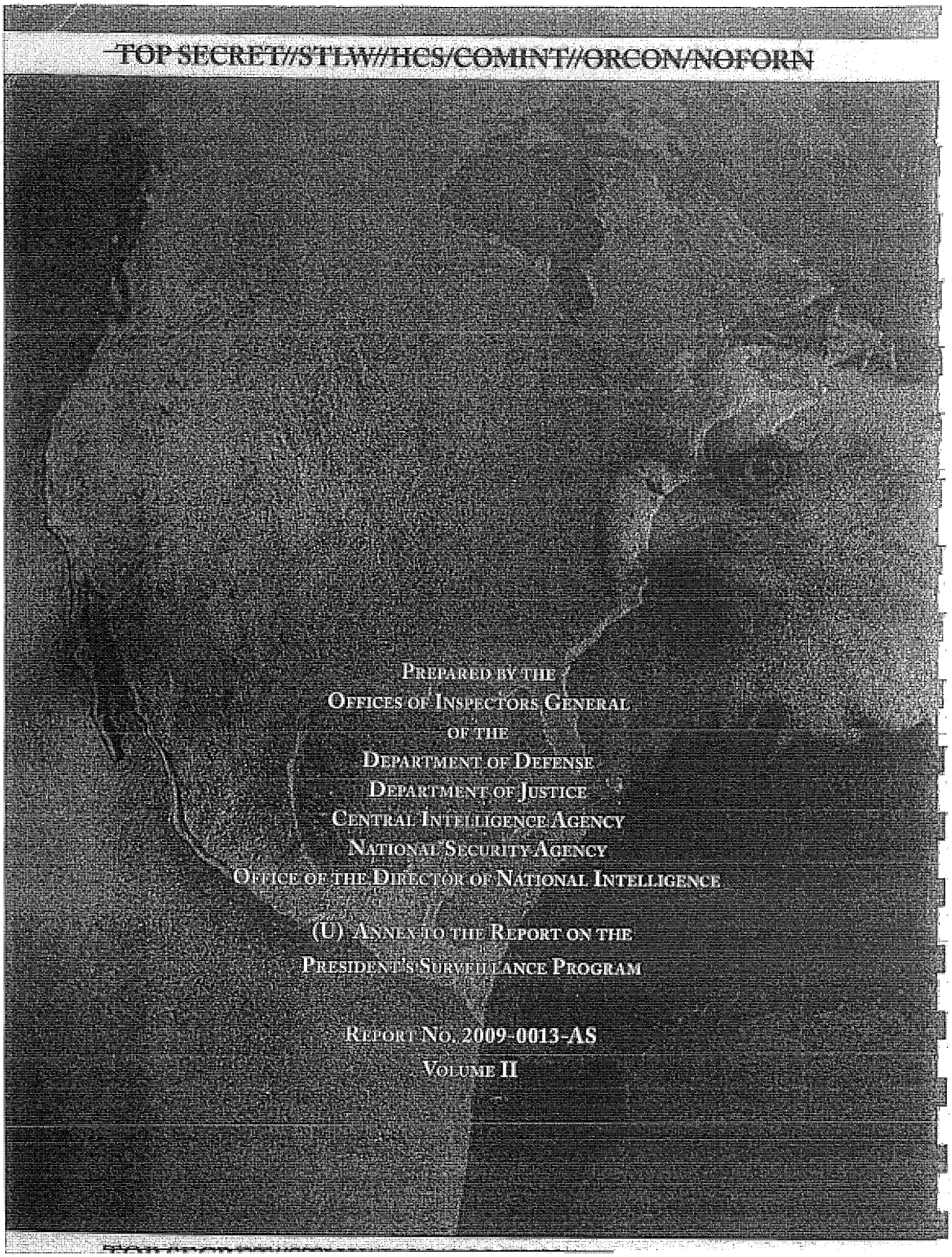
~~(TS//STLW//SI//OC/NF)~~ We found that the ODNI's primary role in the Program was the preparation of 12 ODNI threat assessments approved by the DNI or PDDNI for use in the Program reauthorizations. The ODNI-prepared threat assessments set forth the ODNI's view regarding the existing threat of an al Qaeda terrorist attack against the United States and provided the DNI's recommendation regarding the need to reauthorize the Program. We found that the ODNI threat assessments were drafted by experienced NCTC personnel under the supervision of knowledgeable NCTC supervisors. We noted that the threat assessments were subject to review by OGC and DOJ attorneys before approval. Additionally, we found that the process used by the ODNI to prepare and obtain approval of the threat assessments was straightforward, reasonable, and consistent with the preparation of other documents requiring DNI approval. Overall, we found the ODNI process for the preparation and approval of the threat assessments was responsible and effective.

~~(TS//STLW//SI//OC/NF)~~ We also found that the ODNI oversight components played a limited role in oversight of the Program. The limited ODNI oversight role was due to delays in obtaining Program access for ODNI oversight personnel and to temporary resource limitations related to the stand-up of the agency. However, we believe that the 2008 amendments to EO 12333 and improved staffing levels provide the ODNI oversight components with sufficient resources and authority to fulfill their current oversight responsibilities, assuming timely notification.

This page intentionally left blank.

VI. (U) APPENDIX - STRUCTURE OF THE ODNI – 2005





PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

(U) ANNEX TO THE REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

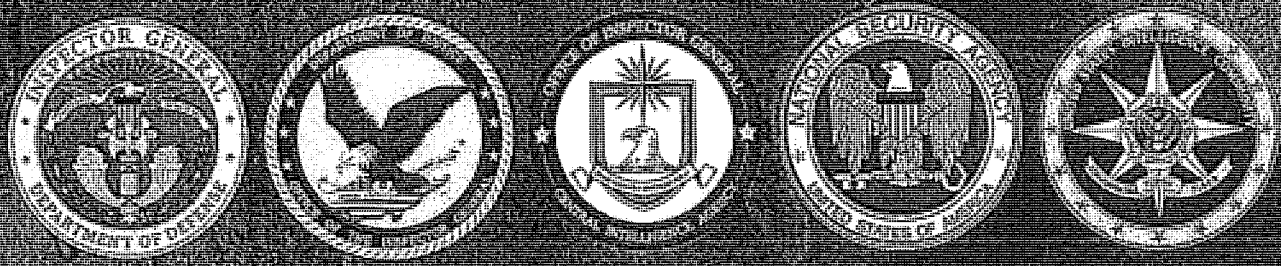
REPORT NO. 2009-0013-AS

VOLUME II

(U) ANNEX TO THE REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

VOLUME III

10 JULY 2009



PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Special Warning

The report contains compartmented, classified material and no secondary distribution may be made without prior consent of the participating Inspectors General. Improper disclosure of this report may result in criminal, civil, or administrative penalties.

REPORT NO. 2009-0013-AS

A Review of the Department of Justice's Involvement with the President's Surveillance Program (U)

Department of Justice
Office of the Inspector General
Oversight and Review Division
July 2009

~~Derived From: NSA/CSS M 1-52, 2-100~~
~~NSA/CSS M 1-52, 12-48~~
~~Dated: 20070108~~
~~Declassify On: 20340713~~

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION (U) 1

I. Methodology of OIG Review (U) 3

II. Organization of this Report (U) 5

CHAPTER TWO: LEGAL AUTHORITIES (U) 7

I. Constitutional, Statutory, and Executive Order Authorities (U) 7

A. Article II, Section 2 of the Constitution (U) 7

B. The Fourth Amendment (U) 7

C. The Foreign Intelligence Surveillance Act (FISA) (U) 8

1. Overview of FISA (U) 8
2. FISA Applications and Orders (U) 10
3. FISA Court (U) 11

D. Authorization for Use of Military Force (U) 12

E. Executive Order 12333 (U) 13

II. Presidential Authorizations (U) 14

A. Types of Collection Authorized ~~(S//NF)~~ 15

B. Findings and Primary Authorities (U) 16

C. The Reauthorization Process (U) 16

D. Approval "as to form and legality" (U) 17

CHAPTER THREE: INCEPTION AND EARLY OPERATION OF STELLAR WIND (SEPTEMBER 2001 THROUGH APRIL 2003) ~~(S//NF)~~ 19

I. Inception of the Stellar Wind Program (U//~~FOUO~~) 19

A. The National Security Agency (U) 19

B. Implementation of the Program (September 2001 through November 2001) ~~(S//NF)~~ 20

1. Pre-Stellar Wind Office of Legal Counsel Legal Memoranda (U) 23
2. Presidential Authorization of October 4, 2001 ~~(TS//SI//NF)~~ 28

C. Presidential Authorization is Revised and the Office of Legal Counsel Issues Legal Memoranda in Support of the Program (November 2001 through January 2002) ~~(TS//STLW//SI//OC/NF)~~ 31

1. Presidential Authorization of November 2, 2001 ~~(TS//SI//NF)~~ 31
2. Yoo Drafts Office of Legal Counsel Memorandum Addressing Legality of Stellar Wind ~~(TS//STLW//SI//OC/NF)~~ 33
3. Additional Presidential Authorizations (U) 38
4. Subsequent Yoo Opinions (U) 39
5. Yoo's Communications with the White House (U) 40
6. Gonzales's View of the Department's Role in Authorizing the Stellar Wind Program ~~(S//NF)~~ 41

II. NSA's Implementation of the Stellar Wind Program (U//~~FOUO~~) 42

A. Implementation of Stellar Wind (U//~~FOUO~~) 42

1. Basket 1 – Telephone and E-Mail Content Collection ~~(TS//STLW//SI//OC/NF)~~ 44
2. Basket 2 – Telephony Meta Data Collection ~~(TS//STLW//SI//OC/NF)~~ 48
3. Basket 3 – E-Mail Meta Data Collection ~~(TS//STLW//SI//OC/NF)~~ 51

B. NSA Process for Analyzing Information Collected Under Stellar Wind ~~(S//NF)~~ 52

1. Basket 1: Content tasking, Analysis, and Dissemination ~~(TS//STLW//SI//OC/NF)~~ 52
2. Baskets 2 and 3: Telephony and E-Mail Meta Data Queries, Analysis, and Dissemination ~~(TS//STLW//SI//OC/NF)~~ 54

III. FBI's Early Participation in the Stellar Wind Program ~~(S//NF)~~ 58

A. FBI Director First Informed of Stellar Wind Program (U//~~FOUO~~) 59

B. [redacted] 59

C. FBI Begins to Receive and Disseminate Stellar Wind "Tippers" ~~(S//NF)~~ 63

1. FBI Initiates [redacted] (S//NF) 63
2. FBI Field Offices' Response to [redacted] Leads ~~(S//NF)~~ 67

b1, b3, b7E

3. FBI's Efforts to Track Stellar Wind Tippers and Update Executive Management on Status of [redacted] Leads ~~(S//NF)~~ 69 b1, b3, b7E

IV. Justice Department Office of Intelligence Policy and Review's (OIPR) and FISA Court's Early Role in Stellar Wind ~~(TS//STLW//SI//OC/NF)~~ 70

A. Overview of OIPR (U) 71

B. OIPR Counsel Learns of Stellar Wind Program (U//~~FOUO~~) 71

C. FISA Court is Informed of Stellar Wind ~~(TS//SI//NF)~~ 74

D. OIPR Implements "Scrubbing" Procedures for Stellar Wind Information in International Terrorism FISA Applications ~~(TS//STLW//SI//OC/NF)~~ 78

1. Initial Scrubbing Procedures ~~(TS//SI//NF)~~ 79
2. Complications with Scrubbing Procedures ~~(TS//SI//NF)~~ 81

E. Judge Kollar-Kotelly Succeeds Judge Lamberth as FISA Court Presiding Judge (U) 83

1. Judge Kollar-Kotelly Modifies OIPR Scrubbing Procedures ~~(TS//SI//NF)~~ 83
2. OIPR implements Judge Kollar-Kotelly's Scrubbing Procedure ~~(TS//SI//NF)~~ 85

V. FBI Initiates Measures to Improve the Management of Stellar Wind Information ~~(S//NF)~~ 88

A. CAU Acting Unit Chief Evaluates FBI Response to Stellar Wind ~~(S//NF)~~ 89

B. FBI Increases Cooperation with NSA and Initiates [redacted] Project to Manage Stellar Wind Information ~~(TS//STLW//SI//OC/NF)~~ 90 b1, b3, b7E

C. FBI Assigns CAU Personnel to NSA on Full-Time Basis ~~(S//NF)~~ 93

VI. OIG Analysis (U) 94

CHAPTER FOUR: LEGAL REASSESSMENT OF STELLAR WIND (MAY 2003 THROUGH MAY 2004) ~~(TS//SI//NF)~~ 99

I. Justice Department Reassesses Legality of Stellar Wind Program ~~(TS//SI//NF)~~ 99

A. Overview of Office of Legal Counsel (U) 99

B. Personnel Changes within Office of Legal Counsel (U) 100

1. Yoo's Role in the Program (October 2001 through May 2003) (U) 100
2. Philbin Replaces Yoo (U) 103
3. Initial Concerns with Yoo's Analysis (U) 104
4. Problems with [redacted] (~~TS//STLW//SI//OC/NF~~) 106
5. Other Collection Concerns (~~S//NF~~) 108
6. Decision to Draft New OLC Memorandum (U) 108

C. Reassessment of Legal Rationale for the Program (~~TS//SI//NF~~) 109

1. Goldsmith Becomes OLC Assistant Attorney General (U) 109
2. NSA Denied Access to OLC Memoranda (U//~~FOUO~~) 111
3. Goldsmith Joins Effort to Reassess Legal Basis for the Program (~~TS//SI//NF~~) 112
4. AUMF Becomes the Primary Legal Rationale Supporting [redacted] of the Stellar Wind Program (~~TS//STLW//SI//OC/NF~~) 113
5. Office of Legal Counsel Raises its Reassessment of the Stellar Wind Program (December 2003 through January 2004) (~~TS//SI//NF~~) 115
6. Deputy Attorney General Comey is Read into the Program (U) 118

D. Office of Legal Counsel Presents its Conclusions to the White House (U) 119

1. March 4, 2004: Comey Meets with Ashcroft to Discuss Problems with the Program (U) 120
2. March 5, 2004: Comey Determines Ashcroft is "Absent or Disabled" (U) 121
3. March 5, 2004: Goldsmith and Philbin Seek Clarification from White House on Presidential Authorizations (U) 122
4. March 6 to 8, 2004: The Department Concludes That Yoo's Legal Memoranda Did Not Cover the Program (U) 124
5. March 9, 2004: White House Seeks to Persuade Department and FBI to Support Continuation of the Program (~~S//NF~~) 126
6. Conflict Ensues between Department and White House (U) 129

II. White House Continues Program without Justice Department's Certification (~~TS//SI//NF~~) 130

A. White House Counsel Gonzales Certifies March 11, 2004, Presidential Authorization ~~(TS//SI//NF)~~ 131

1. March 10, 2004: Office of Legal Counsel Presses for Solicitor General to be Read into Program (U) 131
2. March 10, 2004: Congressional Leaders Briefed on Situation (U) 131
3. March 10, 2004: Hospital Visit (U) 134
4. March 10, 2004: Olson is Read into the Program (U). 140
5. March 11, 2004: Goldsmith Proposes Compromise Solution (U) 141
6. March 11, 2004: White House Asserts that Comey's Status as Acting Attorney General was Unclear (U) 142
7. March 11, 2004: Gonzales Certifies Presidential Authorization as to Form and Legality ~~(TS//SI//NF)~~ . 144

B. Department and FBI Officials React to Issuance of March 11, 2004, Authorization ~~(TS//SI//NF)~~ 148

1. Initial Responses of Department and FBI Officials (U) 149
2. Department and FBI Officials Consider Resigning (U) 152
3. Comey and Mueller Meet with President Bush (U)..... 155
4. Comey Directs Continued Cooperation with NSA (U) .. 157
5. Department Conducts Additional Legal Analysis (U)... 158
6. Comey Determines that Ashcroft Remains "Absent or Disabled" (U) 163
7. Judge Kollar-Kotelly Briefed on Lack of Attorney General Certification (U) 164
8. Comey and Gonzales Exchange Documents Asserting Conflicting Positions (U) 164

C. White House Agrees to [redacted] ~~(TS//STLW//SI//OC/NF)~~ 168

1. March 19, 2004, Modification (U)..... 168
2. [redacted] 172
3. [redacted] 173
4. [redacted] 175
5. Judge Kollar-Kotelly is Presented with the OLC Legal Analysis Regarding [redacted] ~~(TS//STLW//SI//OC/NF)~~..... 175
6. April 2, 2004, Modification (U) 178

b1, b3, b7E

7. [redacted] Standard is Conveyed to the FBI (~~TS//SI//NF~~) 180
8. Office of Legal Counsel Assesses NSA's Compliance with New Collection Standards (~~TS//SI//NF~~) 180
9. May 5, 2004, Presidential Authorization (~~TS//SI//NF~~) 181
10. May 6, 2004, OLC Memorandum (~~TS//SI//NF~~) 182

III. OIG Analysis (U) 186

A. Department's Access to and Legal Review of Stellar Wind Program Through May 2004 (~~TS//SI//NF~~) 186

B. The Hospital Visit (U) 197

C. Recertification of the Presidential Authorization and Modification of the Program (U) 199

CHAPTER FIVE: STELLAR WIND PROGRAM'S TRANSITION TO FISA AUTHORITY (JUNE 2004 THROUGH AUGUST 2007) 203

I. E-Mail Meta Data Collection Under FISA (~~TS//SI//NF~~) 203

A. Application and FISA Court Order (U) 203

1. Decision to Seek a Pen Register and Trap and Trace (PR/TT) Order from the FISA Court (~~TS//SI//NF~~) 203
2. Briefing for Judge Kollar-Kotelly (U) 205
3. The PR/TT Application (~~TS//SI//NF~~) 205
4. Judge Kollar-Kotelly Raises Questions about PR/TT Application (~~TS//SI//NF~~) 212
5. FISA Court Order (U) 213

B. President Orders Limited Use [redacted] (~~TS//STLW//SI//OC/NF~~) 217

1. The President's August 9, 2004, Memorandum to the Secretary of Defense (~~TS//SI//NF~~) 217
2. Office of Legal Counsel Determines [redacted] (~~TS//STLW//SI//OC/NF~~) 218

C. Non-Compliance with PR/TT Order (~~TS//SI//NF~~) 219

1. Filtering Violations (~~TS//SI//NF~~) 219
2. FISA Court Renews PR/TT Order (~~TS//SI//NF~~) 221
3. [redacted] 222

D. Subsequent PR/TT Applications and Orders (~~TS//SI//NF~~) . 224

II. Telephony Meta Data Collection Under FISA (~~TS//SI//NF~~) 225

A. Decision to Seek Order Compelling Production of Call detail records ~~(TS//SI//NF)~~ 226

B. Summary of Department's Application and Related FISA Court Order ~~(S/NF)~~ 228

C. Non-Compliance with Section 215 Orders ~~(TS//SI//NF)~~ 232

III. Content Collection under FISA ~~(TS//SI//NF)~~ 237

A. Decision to Seek Content Order ~~(TS//SI//NF)~~ 237

B. Summary of Department's December 13, 2006, Content Application ~~(TS//SI//NF)~~ 239

C. Judge Howard Grants Application in Part ~~(TS//SI//NF)~~ 245

D. Domestic Selectors Application and Order ~~(TS//SI//NF)~~ 248

E. Last Stellar Wind Presidential Authorization Expires ~~(TS//SI//NF)~~ 250

F. First Domestic and Foreign Selectors FISA Renewal Applications ~~(TS//SI//NF)~~ 251

G. Revised Renewal Application for Foreign Selectors and Order ~~(TS//SI//NF)~~ 255

IV. The Protect America Act and the FISA Amendments Act of 2008 (U) 259

A. The Protect America Act (U) 260

B. The FISA Amendments Act of 2008 (U) 264

V. OIG Analysis (U) 267

CHAPTER SIX: [redacted] ~~(S//NF)~~ 271

I. [redacted] Process ~~(S//NF)~~ 272

II. FBI's Decision to Issue National Security Letters under [redacted] to Obtain Telephone Subscriber Information ~~(S//NF)~~ 277 b1, b3, b7E

III. [redacted] and Scrubbing Process ~~(TS//SI//NF)~~ 284

IV. Impact of Stellar Wind Information on FBI Counterterrorism Efforts ~~(S//NF)~~ 291

A. Stellar Wind/[redacted] Statistics ~~(TS//STLW//SI//OC/NF)~~ 291

B. FBI Field Office Investigations of [redacted] Tippers ~~(S//NF)~~ 296 b1, b3, b7E

C. FBI Statistical Surveys of [redacted] Meta Data Tippers ~~(TS//STLW//SI//OC/NF)~~ 300 b1, b3, b7E

1. Early 2006 Survey of [redacted] Telephony and E-Mail Meta Data Tippers ~~(TS//STLW//SI//OC/NF)~~ 301 b1, b3, b7E
2. January 2006 Survey of [redacted] E-Mail Meta Data Tippers ~~(TS//STLW//SI//OC/NF)~~ 304

D. FBI Judgmental Assessments of Stellar Wind Information ~~(S//NF)~~ 305

E. Examples of FBI Counterterrorism Cases Involving Stellar Wind Information ~~(S//NF)~~ 310

1. [redacted] 311
2. 313
3. 315
4. 318
5. 322

b1, b3, b6, b7C, b7E

V. OIG Analysis (U) 325

CHAPTER SEVEN: DISCOVERY ISSUES RELATED TO STELLAR WIND INFORMATION ~~(TS//SI//NF)~~ 333

I. Relevant Law (U) 333

II. Cases Raise Questions about Government's Compliance with Discovery Obligations (U) 335

A. [redacted] 335

B. 336

b1, b3, b6, b7C, b7E

III. Criminal Division Examines Discovery Issues (U) 340

A. The "Informal Process" for Treating Discovery Issues in International Terrorism Cases (U) 341

B. [redacted] Memorandum Analyzing Discovery Issues Raised by the Stellar Wind Program ~~(TS//STLW//SI//OC/NF)~~ 342

C. Office of Legal Counsel and Discovery Issue (U) 346

IV. Use of the Classified Information Procedures Act (CIPA) to Respond to Discovery Requests (U) 347

A. Overview of CIPA (U) 348

B. Use of CIPA in International Terrorism Prosecutions Alleged to Involve Stellar Wind-Derived Information ~~(TS//STLW//SI//OC/NF)~~ 348

C. Government Arguments in Specific Cases (U) 351

[redacted] 351 b1, b3,
..... 353 b6,
..... 354 b7C,
..... 355 b7E

V. OIG ANALYSIS (U) 357

CHAPTER EIGHT: PUBLIC STATEMENTS ABOUT THE SURVEILLANCE PROGRAM (U) 361

I. Summary of the Dispute about the Program (U) 361

II. The New York Times Articles and President Bush's Confirmation Regarding NSA Activities (U) 363

III. Other Administration Statements (U) 365

IV. Testimony and Other Statements (U) 366

A. Gonzales's February 6, 2006, Senate Judiciary Committee Testimony (U) 367

B. Comey's May 15, 2007, Senate Judiciary Committee Testimony (U) 370

C. Gonzales's June 5, 2007, Press Conference (U) 371

D. Gonzales's July 24, 2007, Senate Judiciary Committee Testimony (U) 371

E. FBI Director Mueller's July 26, 2007, House Committee on the Judiciary Testimony (U) 376

F. Gonzales's Follow-up Letter to the Senate Judiciary Committee (U) 377

V. OIG Analysis (U) 378

CHAPTER NINE: CONCLUSIONS (U) 387

I. Operation of the Program (U//~~FOUO~~) 388

II. Office of Legal Counsel's Analysis of the Stellar Wind Program ~~(TS//SI//NF)~~ 389

III. Hospital Visit and White House Recertification of the Program (U) 394

IV. Transition of Program to FISA Authority ~~(TS//STLW//SI//OC/NF)~~ 396

V. Impact of Stellar Wind Information on FBI Counterterrorism Efforts ~~(S//NF)~~ 397

VI. Discovery and "Scrubbing" Issues ~~(TS//SI//NF)~~ 402

VII. Gonzales's Statements (U) 404

VIII. Conclusion (U) 406

CHAPTER ONE
INTRODUCTION (U)

On October 4, 2001, three weeks after the terrorist attacks of September 11, 2001, the President issued a Top Secret Presidential Authorization to the Secretary of Defense directing that the signals intelligence capabilities of the National Security Agency (NSA) be used to detect and prevent further attacks in the United States. The Presidential Authorization stated that an extraordinary emergency existed permitting the use of electronic surveillance within the United States for counterterrorism purposes, without a court order, under certain circumstances. For over 6 years, this Presidential Authorization was renewed at approximately 30 to 45 day intervals to authorize the highly classified NSA surveillance program, which was given the cover term "Stellar Wind."[1] ~~(TS//STLW//SI//OC/NF)~~

Under these Presidential Authorizations and subsequently obtained Foreign Intelligence Surveillance Court (FISA Court) orders, the NSA intercepted the content of international telephone and e-mail communications of both U.S. and non-U.S. persons when certain criteria were met. In addition, the NSA collected vast amounts of telephony and e-mail meta data – that is, communications signaling information showing contacts between and among telephone numbers and e-mail addresses, but not including the contents of the communications. [redacted].[2] ~~(TS//STLW//SI//OC/NF)~~

Within the Department of Justice (Department or Justice Department) and the Intelligence Community, the different types of information collected under the NSA program came to be referred to as three different "baskets" of information. The collection of the content of telephone and e-mail

---

[1] This program is also known as the President's Surveillance Program (PSP). In Title III of the Foreign Intelligence Surveillance Act Amendments Act of 2008 (FISA Amendments Act), the President's Surveillance Program is defined as

> the intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005 (commonly known as the Terrorist Surveillance Program).

FISA Amendments Act, Title III, Sec. 301(a)(3). (U)

[redacted]

communications was referred to as basket 1. The collection of telephone meta data – including information on the date, time, and duration of the telephone call, the telephone number of the caller, and the number receiving the call – was referred to as basket 2. The collection of e-mail meta data – including the "to," "from," "cc," "bcc," and "sent" lines of an e-mail, but not the "subject" line or content of the e-mail – was referred to as basket 3. ~~(TS//STLW//SI//OC/NF)~~

The content and meta data information was used by the NSA, working with other members of the Intelligence Community, to generate intelligence reports. [redacted] By March 2006, over [redacted] individual U.S. telephone numbers and [redacted] e-mail addresses had been "tipped" to the FBI as leads, the vast majority of which were disseminated to FBI field offices for investigation or other action. Some Stellar Wind-derived information also was disseminated to the larger Intelligence Community through traditional intelligence reporting channels.[3] ~~(TS//STLW//SI//OC/NF)~~

In addition to the FBI's receipt of information from the program, the Justice Department was involved in the program in other ways. Most significantly, the Department's Office of Legal Counsel (OLC) provided advice to the White House and the Attorney General on the overall legality of the Stellar Wind program. In addition, the Department's Office of Intelligence Policy and Review (now called the Office of Intelligence in the Department's National Security Division) worked with the FBI and NSA to justify the inclusion of Stellar Wind-derived information in applications seeking orders under the Foreign Intelligence Surveillance Act (FISA), and when unable to do so, to exclude such information from the applications. The Department's National Security Division (NSD) also submitted classified *ex parte* legal filings in federal courts to address any Stellar Wind reporting concerning defendants during discovery in international terrorism prosecutions. ~~(TS//STLW//SI//OC/NF)~~

Beginning in December 2005, aspects of the Stellar Wind program were publicly disclosed in media reports, originally in a series of articles by The New York Times. After these articles disclosed the telephone and e-mail content collection (basket 1), the President, Attorney General Alberto Gonzales, and other Administration officials publicly confirmed the

[3] The larger Intelligence Community also includes components within other Departments, such as the Departments of Homeland Security, Treasury, Defense, and State. (U)

existence of this part of the program. However, the other aspects of the program – the collection of telephone and e-mail meta data – have not been publicly confirmed. ~~(TS//STLW//SI//OC/NF)~~

The President and other Administration officials labeled the NSA collection of information that was publicly disclosed as "the Terrorist Surveillance Program," although this name was sometimes used within the Intelligence Community to refer to the entire Stellar Wind program. The program was also referred to by other names, such as the "Warrantless Wiretapping Program" or the "NSA Surveillance Program." As discussed above, the technical name for the program, and the term we generally use throughout this report, is the Stellar Wind program.[4] ~~(S//NF)~~

This report describes the Office of the Inspector General's (OIG) review of the Department's role in the Stellar Wind program. Our review discusses the evolution of the Stellar Wind program, including the changes in the Department's legal analyses of the program, the operational changes to the program, and the eventual transition of the program from presidential authority to statutory authority under FISA. The report also assesses the FBI's use of information derived from the Stellar Wind program, including the impact of the information in FBI counterterrorism investigations. ~~(TS//STLW//SI//OC/NF)~~

I. Methodology of OIG Review (U)

During the course of this review, the OIG conducted approximately 80 interviews. Among the individuals we interviewed were former White House Counsel and Attorney General Gonzales; former Deputy Attorney General James Comey; former NSA Director Michael Hayden; FBI Director Robert Mueller, III; former Counsel for Intelligence Policy James Baker; former Assistant Attorneys General for OLC Jay Bybee and Jack Goldsmith; former Principal Deputy and Acting Assistant Attorney General for OLC Steven Bradbury; former Deputy Assistant Attorney General for OLC and Associate Deputy Attorney General Patrick Philbin; and former Assistant Attorneys General for the NSD Kenneth Wainstein and Patrick Rowan. We also interviewed senior FBI Counterterrorism Division officials, the FBI General Counsel and other FBI attorneys, FBI special agents and intelligence analysts, and senior officials in the Department's Criminal and National Security Divisions.[5] (U)

---

[4] Stellar Wind is classified as a Top Secret/Sensitive Compartmented Information program. ~~(S//NF)~~

[5] Although the FBI is a component of the Department of Justice, references in this report to Department officials generally mean non-FBI Department officials. This

(Cont'd.)

We attempted to interview former Attorney General John Ashcroft, but he declined our request for an interview. (U)

In addition, we attempted to interview former Deputy Assistant Attorney General for OLC John Yoo, who drafted the early legal memoranda supporting the legality of the Stellar Wind program. Yoo, through his counsel, declined our request for an interview. ~~(TS//SI//NF)~~

We also attempted to interview White House officials regarding the program, including Andrew Card, former Chief of Staff to President George W. Bush. We made our request for an interview of Card both directly to Card and through the Office of the Counsel to the President (White House Counsel's Office). Card did not grant our request for an interview. Similarly, we attempted to interview David Addington, former Counsel to Vice President Richard B. Cheney. We contacted the Office of the Vice President, but that office did not respond to our request for an interview of Addington. (U)

We believe that we were able to obtain a full picture of the evolution of the program and the theories supporting its legality. However, the refusal by White House officials, former Attorney General Ashcroft, and former Deputy Assistant Attorney General Yoo to be interviewed hampered our ability to fully investigate the process by which the White House and the Justice Department arrived at the initial legal rationale to support the program. In addition, because of our inability to interview Ashcroft, we could not fully determine what efforts the Department took to press the White House for additional Department attorneys to be read into Stellar Wind to work on the legal analysis of the program during its first two years of operation. ~~(TS//SI//NF)~~

In our review, we also examined thousands of electronic and hard copy documents, including the Presidential Authorizations and threat assessments, OLC legal memoranda supporting the program, contemporaneous notes and e-mails of various senior Department and FBI officials, and FISA Court pleadings and orders. We also reviewed NSA materials, including NSA OIG reports on the Stellar Wind program and correspondence between the NSA Office of General Counsel and the Department. ~~(TS//SI//NF)~~

In addition, we received from the FBI an electronic database of its collection of Electronic Communications (EC) that were used to disseminate

---

distinction is especially relevant to our discussion of the number of Department personnel read into the Stellar Wind program, as distinguished from the number of FBI personnel read into the program. (U//~~FOUO~~)

Stellar Wind-derived leads to FBI field offices. This database contained approximately [redacted] ECs, including leads to the FBI's 56 field offices, and responses from those field offices, among other documents. The OIG used this database to confirm information it obtained through interviews and to assist in our analysis of FBI investigations that were based on Stellar Wind information. ~~(TS//STLW//SI//OC/NF)~~

II. Organization of this Report (U)

Chapter Two of this report provides an overview of the primary legal authorities that are relevant to the Stellar Wind program. This chapter also discusses the Presidential Authorizations that were issued to approve the program. (U//~~FOUO~~)

Chapter Three describes the inception and early implementation of the Stellar Wind program from September 2001 through April 2003. This chapter includes a description of the early OLC legal memoranda on the legality of Stellar Wind, how the program was technically implemented, the FBI's early participation in the program, and the FISA Court's first awareness of the program. ~~(TS//SI//NF)~~

Chapter Four covers the period from May 2003 through May 2004 when the legal rationale for the program was substantially reconsidered by the Justice Department. This chapter details in particular the events of March 2004 when the White House decided to continue the program without the Department's certification of a Presidential Authorization. During this time, Attorney General Ashcroft was hospitalized and Deputy Attorney General Comey temporarily exercised the powers of the Attorney General in his capacity as Deputy Attorney General. Comey declined to recertify the Presidential Authorization approving the program based on legal advice he received from OLC Assistant Attorney General Jack Goldsmith, who questioned the adequacy of the legal support for aspects of the program. Comey's decision prompted a significant dispute between the White House and the Justice Department, which resulted in White House Counsel Gonzales and White House Chief of Staff Card visiting Ashcroft in his hospital room in an unsuccessful attempt to have Ashcroft recertify the program. This chapter also describes the background to the dispute, the events related to the hospital visit, the threat by Department officials to resign over the dispute, and the eventual resolution of the dispute. ~~(TS//SI//NF)~~

Chapter Five discusses the transition, in stages, from a program based on Presidential Authorizations to collection activities authorized under the FISA statute. This transition took place in stages between July 2004 and January 2007. This chapter also summarizes legislation in 2007

and 2008 designed to modernize certain provisions of FISA. ~~(TS//STLW//SI//OC/NF)~~

Chapter Six discusses the use of Stellar Wind information by the FBI. It describes the process by which the FBI disseminated Stellar Wind-derived leads to FBI field offices under a program called [redacted] as well as the impact and effectiveness of the Stellar Wind program to the FBI's counterterrorism efforts. ~~(TS//STLW//SI//OC/NF)~~

Chapter Seven examines the Department's handling of discovery issues related to Stellar Wind-derived information in international terrorism prosecutions. ~~(TS//STLW//SI//OC/NF)~~

Chapter Eight analyzes testimony and public statements about aspects of the Stellar Wind program by Attorney General Gonzales. We assess whether the Attorney General's statements, particularly his testimony to the Senate Judiciary Committee in February 2006 and July 2007, were false, inaccurate, or misleading. ~~(S//NF)~~

Chapter Nine contains our conclusions and recommendations. (U)

CHAPTER TWO
LEGAL AUTHORITIES (U)

This chapter summarizes the primary legal authorities referred to throughout this report concerning the Stellar Wind program. These authorities include Article II, Section 2 of the Constitution; the Fourth Amendment to the Constitution; the Foreign Intelligence Surveillance Act; the Authorization for Use of Military Force Joint Resolution (AUMF) passed by Congress after the terrorist attacks of September 11, 2001; Executive Order 12333; and the Presidential Authorizations specifically authorizing the Stellar Wind program. Other authorities, including relevant criminal statutes and judicial opinions, are discussed throughout the report. ~~(TS//SI//NF)~~

I. Constitutional, Statutory, and Executive Order Authorities (U)

A. Article II, Section 2 of the Constitution (U)

Article II, Section 2 of the Constitution, which was one of the primary authorities cited in the Presidential Authorizations in support of the legality of the Stellar Wind program, provides in relevant part:

> The President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service of the United States; he may require the Opinion, in writing, of the principal Officer in each of the executive Departments, upon any Subject relating to the Duties of their respective Offices . . . . ~~(TS//SI//NF)~~

B. The Fourth Amendment (U)

The Fourth Amendment to the Constitution, which also was raised as an important factor in the analysis of the legality of the Stellar Wind program, provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized. ~~(TS//SI//NF)~~

C. The Foreign Intelligence Surveillance Act (FISA)[6] (U)

The Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801, et seq., was enacted in 1978 to "provide legislative authorization and regulation for all electronic surveillance conducted within the United States for foreign intelligence purposes." S. Rep. No. 95-701, at 9 (1978), reprinted in 1978 U.S.C.C.A.N. 3973, 3977. Three major FISA issues are covered in this report. First, as discussed in Chapter Four, FISA was central to a controversy that arose in late 2003 and early 2004 when officials in the Office of Legal Counsel (OLC) and others viewed FISA as potentially in conflict with the legal rationale for at least one aspect of the Stellar Wind program. OLC officials reasoned that if courts viewed FISA in isolation, they might conclude that Congress intended to regulate the President's power to conduct electronic surveillance during wartime, thereby raising questions about the legality of aspects of the program. ~~(TS//STLW//SI//OC/NF)~~

Second, after the FISA Court was informed about the Stellar Wind program in January 2002, it required the government to carefully scrutinize each FISA application to ensure that no Stellar Wind-derived information was relied upon in support of a FISA application without the Court's knowledge, and later without its consent. This process, known as "scrubbing," is discussed in Chapters Three and Six.
~~(TS//STLW//SI//OC/NF)~~

Third, beginning in July 2004, the Stellar Wind program was brought under FISA authority in stages, with the entire program brought under FISA authority by January 2007. In August 2007 and again in July 2008, FISA was amended, and [redacted] The migration of the Stellar Wind program from presidential authority to FISA authority, as well as legislation subsequently enacted to modernize FISA, is discussed in Chapter Five.
~~(TS//STLW//SI//OC/NF)~~

In the following sections, we summarize relevant provisions of FISA as they related to the Stellar Wind program. ~~(TS//SI//NF)~~

1. Overview of FISA (U)

FISA authorizes the federal government to engage in electronic surveillance and physical searches, to use pen register and trap and trace

---

[6] Unless otherwise indicated, all references to FISA are to the statute as it existed prior to the Protect America Act of 2007 and the FISA Amendments Act of 2008. (U)

devices, and to obtain business records to acquire inside the United States foreign intelligence information by, in some instances, targeting foreign powers and agents of foreign powers.[7] FISA also permits the targeting of foreign powers and their agents who are located outside the United States. As a general rule, the FISA Court must first approve an application by the government before the government initiates electronic surveillance. FISA applications must identify or describe the "target" of the surveillance, and must establish probable cause to believe that the target is a "foreign power" or "agent of a foreign power" and that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power."[8] 50 U.S.C. § 1804(a)(4)(A) & (B). ~~(TS//SI//NF)~~

FISA provides four exceptions to the requirement of obtaining judicial approval prior to conducting electronic surveillance: (1) for electronic surveillance directed at certain facilities where the Attorney General certifies that the electronic surveillance is solely directed at communications transmitted by means used exclusively between or among foreign powers or from property under the open and exclusive control of a foreign power, 50 U.S.C. § 1802; (2) where the Attorney General determines an emergency exists and authorizes emergency surveillance until the information sought is obtained, the after-filed application for an order is denied, or the expiration of 72 hours from the time of Attorney General authorization, 50 U.S.C. § 1805(f); (3) for training and testing purposes, 50 U.S.C. § 1805(g); and (4) for 15 days following a congressional declaration of war, 50 U.S.C. § 1811.[9] (U)

The 15-day war declaration exception to FISA's warrant requirement was particularly relevant to the events of 2004, when OLC reassessed its prior opinions concerning the legality of the Stellar Wind program. ~~(TS//SI//NF)~~

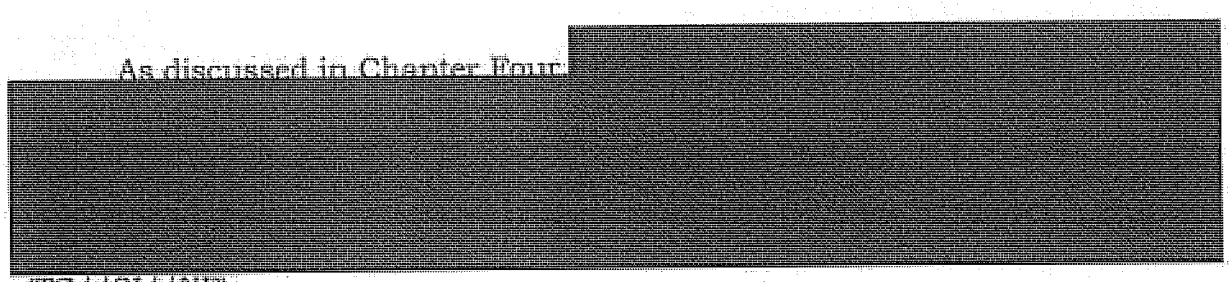
---

[7] This report is primarily concerned with the provisions of FISA that authorize electronic surveillance, pen register and trap and trace devices, and access to certain business records. ~~(TS//SI//NF)~~

[8] The terms "foreign power" and "agent of a foreign power" are defined in FISA at 50 U.S.C. § 1801(a) & (b). "Foreign power" is defined, inter alia, as "a group engaged in international terrorism or activities in preparation therefor; . . . ." 50 U.S.C. § 1801(a)(4). An "agent of a foreign power" may be a U.S. person, defined at 50 U.S.C. § 1801(i) to mean, inter alia, a United States citizen or permanent resident alien. The term "facilities" is not defined in FISA. (U)

[9] The Attorney General's emergency surveillance authority under 50 U.S.C. § 1805(f) was extended to 7 days under Section 105(a) of the FISA Amendments Act of 2008. (U)

As discussed in Chapter Four,



~~(TS//SI//NF)~~

Another FISA provision prohibits persons from intentionally engaging in electronic surveillance "under color of law except as authorized by statute[.]" 50 U.S.C. § 1809(a)(1). As discussed in Chapter Eight, in 2006 the Justice Department asserted in a publicly released legal analysis that this provision did not preclude certain warrantless electronic surveillance activities because such surveillance was "authorized by" subsequent legislative enactments – principally the AUMF. The Department also asserted that the AUMF "confirms and supplements the President's constitutional authority" to conduct warrantless electronic surveillance against the enemy during wartime. (U)

2. FISA Applications and Orders (U)

FISA applications were presented to the FISA Court by the Department's Office of Intelligence Policy and Review (OIPR).[10] Department and FBI officials familiar with the preparation and presentation of FISA applications described this process as extremely time-consuming and labor intensive. (U)

Each application must be approved and signed by the Attorney General (or Acting Attorney General) or Deputy Attorney General and must include the certification of a federal officer identifying or describing the target of the electronic surveillance; a "statement of the facts and circumstances relied upon by the applicant to justify his belief" that the target is a foreign power or agent of a foreign power and that the electronic surveillance is directed at the facilities or places used or to be used by the target; a statement of proposed minimization procedures; and a detailed description of the nature of the information sought and the type of communication or activities to be subjected to the surveillance. 50 U.S.C. § 1804(a)(1)-(6).[11] The application must also include the certification of a

---

[10] The Office of Intelligence Policy and Review became a part of the Department's National Security Division, which was created in September 2006. As of April 2008, the Office of Intelligence Policy and Review was renamed the Office of Intelligence. This organizational change did not affect the FISA application process. (U)

[11] FISA defines minimization procedures as

> [s]pecific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the

(Cont'd.)

high-ranking executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense that the information sought is deemed to be foreign intelligence information, that such information "cannot reasonably be obtained by normal investigative techniques," and that a "significant purpose" of the surveillance is to obtain foreign intelligence information.[12] Id. at § 1804(a)(7). (U)

FISA orders authorize electronic surveillance of U.S. persons for 90 days. FISA orders may be renewed upon the same basis as the underlying order. 50 U.S.C. § 1805(e). As noted, FISA also provides for the emergency use of electronic surveillance. When the Attorney General reasonably determines that an emergency situation exists, the use of electronic surveillance may be approved for a period of up to 72 hours (and under the FISA Amendments Act of 2008, up to 7 days) without a FISA order. 50 U.S.C. § 1805(f). (U)

3. FISA Court (U)

The FISA statute established the FISA Court to review applications and issue orders. The FISA Court initially was composed of seven U.S. District Court judges designated by the Chief Justice of the U.S. Supreme Court to serve staggered, non-renewable 7-year terms.[13] 50 U.S.C.

---

particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information . . . .

50 U.S.C. § 1801(h)(1). (U)

[12] As initially enacted, FISA required officials to certify that "the purpose" of the surveillance was to obtain "foreign intelligence information." However, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the USA PATRIOT Act) was enacted in October 2001 and amended this language in FISA to require only that officials certify that "a significant purpose" of the surveillance was to obtain foreign intelligence information. 50 U.S.C. § 1804(a)(7)(B). This amendment, along with post-September 11 changes to Attorney General guidelines on intelligence sharing procedures and a ruling by the FISA Court of Review, removed the so-called "wall" that had existed between intelligence-gathering activities and criminal investigations. See Memorandum from the Attorney General to Director of the FBI, et al., entitled "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI" (March 6, 2002); *In re Sealed Case*, 310 F.3d 717, 727 (For. Int. Surv. Ct. Rev. 2002)(FISA did not "preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution."). (U)

[13] To achieve staggered terms, the initial appointments ranged from one to seven years. 50 U.S.C. § 1803(d). (U)

§ 1803(a) & (d). The number of judges serving on the FISA Court was increased to 11 by the USA PATRIOT Act of 2001. (U)

D. Authorization for Use of Military Force (U)

On September 18, 2001, in response to the terrorist attacks of September 11, Congress approved an Authorization for Use of Military Force Joint Resolution (AUMF). In conjunction with the President's Commander-in-Chief authority under Article II of the Constitution, this legislation has been cited in support of the President's authority to conduct electronic surveillance without judicial approval. See, e.g., Legal Authorities Supporting the Activities of the National Security Agency Described by the President, January 19, 2006 (Justice Department White Paper), at 6-17. The AUMF states, in pertinent part:

> To authorize the use of the United States Armed Forces against those responsible for the recent attacks launched against the United States.
>
> Whereas, on September 11, 2001, acts of treacherous violence were committed against the United States and its citizens; and
>
> Whereas, such acts render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both at home and abroad; and
>
> Whereas, in light of the threat to the national security and foreign policy of the United States posed by these grave acts of violence; and
>
> Whereas, such acts continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States; and
>
> Whereas, the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States: Now, therefore, be it
>
> Resolved by the Senate and House of Representatives of the United States of America in Congress assembled,
>
> . . .
>
> SEC. 2. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES
>
> (a) IN GENERAL – That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or

persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons. (U)

Pursuant to this authority, the President ordered the U.S. armed forces to invade Afghanistan to combat al Qaeda terrorists and overthrow the Taliban government that had given them refuge. (U)

In 2004, OLC took the position that the AUMF was "expressly designed to authorize whatever military actions the Executive deems appropriate to safeguard the United States[,]" including the use of electronic surveillance to detect and prevent further attacks. See Office of Legal Counsel Memorandum, May 6, 2004, at 31, citing 50 U.S.C. § 1811. In addition, the Justice Department asserted in the 2006 White Paper that in enacting FISA Congress contemplated that a later legislative enactment could authorize electronic surveillance outside the procedures set forth in FISA itself, and cited the AUMF as such a legislative enactment. See Justice Department White Paper at 20-28, citing 50 U.S.C. § 1809(a)(1). ~~(TS//STLW//SI//OC/NF)~~

E. Executive Order 12333 (U)

On December 4, 1981, President Reagan signed Executive Order 12333 as part of a series of legal reforms that followed abuses of intelligence-gathering authority documented by the Church Commission in the 1970s.[14] Executive Order 12333 placed restrictions on intelligence collection activities engaged in by Executive Branch agencies, including the NSA, while also seeking to foster "full and free exchange of information" among these agencies.[15] Executive Order 12333 at 1.1. (U)

Executive Order 12333 provides that the Attorney General is authorized "to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power." Id. at 2.5. Executive Order 12333 also provides that

---

[14] See http://www.aarclibrary.org/publib/church/reports/contents.htm. Volumes 5 and 6 of the Church Commission report address abuses of intelligence-gathering authority by the NSA and the FBI. (U)

[15] Executive Order 12333 was amended on July 30, 2008, by Executive Order 13470. This report refers to Executive Order 12333 as it existed prior to that amendment. (U)

electronic surveillance, as defined under FISA, must be conducted in accordance with FISA.[16] (U)

Executive Order 12333 prohibits the collection of foreign intelligence information by "authorized [agencies] of the Intelligence Community . . . for the purpose of acquiring information concerning the domestic activities of United States persons." Id. at 2.3(b). (U)

However, in authorizing the Stellar Wind program, [redacted] As discussed previously, the legal rationale advanced for this exemption was that the Authorization for Use of Military Force and the President's Commander-in-Chief powers gave the President the authority to collect such information, notwithstanding the FISA statute. ~~(TS//STLW//SI//OC/NF)~~

II. Presidential Authorizations (U)

The Stellar Wind program was first authorized by the President on October 4, 2001, and periodically reauthorized by the President through a series of documents issued to the Secretary of Defense entitled "Presidential Authorization for Specified Electronic Surveillance Activities During a Limited Period to Detect and Prevent Acts of Terrorism Within the United States" (Presidential Authorization or Authorization). A total of 43 Presidential Authorizations, not including modifications and related presidential memoranda, were issued over the duration of the program from October 2001 through February 2007.[17] Each Authorization directed the

---

[16] Prior to September 11, 2001, Executive Order 12333 and FISA were generally viewed as the principal governing authorities for conducting electronic surveillance. For example, in 2000 the NSA reported to Congress that

> (U) The applicable legal standards for the collection, retention, or dissemination of information concerning U.S. persons reflect a careful balancing between the needs of the government for such intelligence and the protection of the rights of U.S. persons, consistent with the reasonableness standard of the Fourth Amendment, as determined by factual circumstances.
>
> (U) In the Foreign Intelligence Surveillance Act (FISA) and Executive Order (E.O.) 12333, Congress and the Executive have codified this balancing. (Citations omitted.)

NSA Report to Congress, *Legal Standards for the Intelligence Community in Conducting Electronic Surveillance* (2000). (U)

[17] The Presidential Authorizations were issued on the following dates: October 4, 2001; November 2, 2001; November 30, 2001; January 9, 2002; March 14, 2002; April 18, 2002; May 22, 2002; June 24, 2002; July 30, 2002; September 10, 2002; October 15, 2002; November 18, 2002; January 8, 2003; February 7, 2003; March 17, 2003; April 22, (Cont'd.)

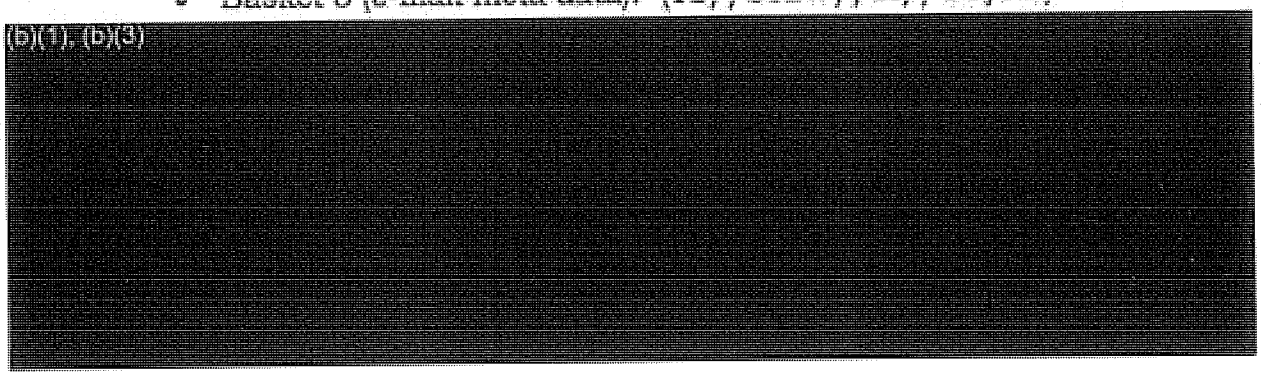
Secretary of Defense to "use the capabilities of the Department of Defense, including but not limited to the signals intelligence capabilities of the National Security Agency, to collect foreign intelligence by electronic surveillance," provided the surveillance met certain criteria. The specific criteria are described in detail in Chapters Three and Four of this report. ~~(TS//STLW//SI//OC/NF)~~

A. Types of Collection Authorized ~~(S//NF)~~

The scope of collection permitted under the Presidential Authorizations varied over time, but generally involved intercepting the content of certain telephone calls and e-mails, and the collection of bulk telephone and e-mail meta data. The term "meta data" has been described as "information about information." As used in the Stellar Wind program, for telephone calls, meta data generally refers to "dialing-type information" (the originating and terminating telephone numbers, and the date, time, and duration of the call), but not the content of the call. For e-mails, meta data generally refers to the "to," "from," "cc," "bcc," and "sent" lines of an e-mail, but not the "subject" line or content. ~~(TS//STLW//SI//OC/NF)~~

The information collected through the Stellar Wind program fell into three categories, often referred to as "baskets":

- Basket 1 (content of telephone and e-mail communications);
- Basket 2 (telephony meta data); and
- Basket 3 (e-mail meta data). ~~(TS//STLW//SI//OC/NF)~~



2003; June 11, 2003; July 14, 2003; September 10, 2003; October 15, 2003; December 9, 2003; January 14, 2004; March 11, 2004; May 5, 2004; June 23, 2004; August 9, 2004; September 17, 2004; November 17, 2004; January 11, 2005; March 1, 2005; April 19, 2005; June 14, 2005; July 26, 2005; September 10, 2005; October 26, 2005; December 13, 2005; January 27, 2006; March 21, 2006; May 16, 2006; July 6, 2006; September 6, 2006; October 24, 2006; and December 8, 2006. The last Presidential Authorization expired February 1, 2007. There were also two modifications of a Presidential Authorization and one Presidential memorandum to the Secretary of Defense issued in connection with the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

B. Findings and Primary Authorities (U)

In this section, we describe certain features common to all the Presidential Authorizations. Each of the Presidential Authorizations included a finding to the effect that terrorist groups of global reach possessed the intent and capability to attack the United States, that an extraordinary emergency continued to exist, and that these circumstances "constitute an urgent and compelling governmental interest permitting electronic surveillance within the United States for counterterrorism purposes, without a court order." ~~(TS//STLW//SI//OC/NF)~~

The primary authorities cited for the legality of these electronic surveillance and related activities were Article II of the Constitution and the Authorization for Use of Military Force Joint Resolution. The Authorizations further provided that any limitation in Executive Order 12333 or any other Presidential directive inconsistent with the Presidential Authorizations shall not apply, to the extent of the inconsistency, to the electronic surveillance authorized under the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

Each Authorization also included the President's determination that to assist in preserving the secrecy necessary to "detect and prevent acts of terrorism against the United States," the Secretary of Defense was to defer notification of the Authorizations outside of the Executive Branch and the activities carried out pursuant to them. The President also noted his intention to inform appropriate members of the Senate and the House of Representatives of the program "as soon as I judge that it can be done consistently with national defense needs." Some Presidential Authorizations described briefings given to members of Congress and FISA Court judges. ~~(TS//STLW//SI//OC/NF)~~

C. The Reauthorization Process (U)

The Presidential Authorizations were issued at intervals of approximately 30 to 45 days. Department officials told the OIG that the intervals were designed to be somewhat flexible to assure the availability of the principals that had to sign the Authorizations and to reassess the reasonableness of the collection.[18] Steven Bradbury, former Principal Deputy and Acting Assistant Attorney General for the Office of Legal Counsel (OLC), said that the main reason for periodically reauthorizing the program was to ensure that the Presidential Authorizations were reviewed frequently to assess the continued need for the program and the program's

[18] The officials who signed the Authorizations included the Attorney General, the President, and the Secretary of Defense (or other high-ranking Department of Defense official). (U//~~FOUO~~)

value. As the period for each Presidential Authorization drew to a close, the Director of Central Intelligence (DCI), and as of June 3, 2005, the Director of National Intelligence (DNI) prepared a threat assessment memorandum for the President describing potential terrorist threats to the United States and outlining intelligence gathered through the Stellar Wind program and other means during the previous Authorization period. The DCI (and later the DNI) and the Secretary of Defense reviewed these memoranda and signed a recommendation that the program be reauthorized.
~~(TS//STLW//SI//OC/NF)~~

Each recommendation was then reviewed by the OLC to assess whether, based on the threat assessment and information gathered from other sources, there was "a sufficient factual basis demonstrating a threat of terrorist attacks in the United States for it to continue to be reasonable under the standards of the Fourth Amendment for the President to [continue] to authorize the warrantless searches involved" in the program. The OLC then advised the Attorney General whether the constitutional standard of reasonableness had been met and whether the Presidential Authorization could be certified "as to form and legality."
~~(TS//STLW//SI//OC/NF)~~

D. Approval "as to form and legality" (U)

As noted above, the Presidential Authorizations were "[a]pproved as to form and legality" by the Attorney General or other senior Department official, typically after the review and concurrence of the OLC. The lone exception to this practice was the March 11, 2004, Authorization which we discuss in Chapter Four. ~~(TS//SI//NF)~~

However, there was no legal requirement that the Authorizations be certified by the Attorney General or other Department official. Former senior Department official Patrick Philbin told us he thought one purpose for the certification was to give the program a sense of legitimacy so that it not "look like a rogue operation."

[redacted] Bradbury told us that the Justice Department certifications served as official confirmation that the Department had determined that the activities carried out under the program were lawful.
~~(TS//STLW//SI//OC/NF)~~

Former Attorney General Gonzales told us that certification of the program as to form and legality was not required as a matter of law, but he believed that it "added value" to the Authorization for three reasons. First,

he said that the NSA was being asked to do something it had not done before, and it was important to assure the NSA that the Attorney General had approved the legality of the program. [redacted] Third, for "purely political considerations" the Attorney General's approval of the program would have value "prospectively" in the event of congressional or Inspector General reviews of the program. ~~(TS//STLW//SI//OC/NF)~~

CHAPTER THREE
INCEPTION AND EARLY OPERATION OF STELLAR WIND (SEPTEMBER 2001 THROUGH APRIL 2003) ~~(S//NF)~~

This chapter describes the early operation of the Stellar Wind program. The five sections of the chapter cover the time period from September 2001 to April 2003. ~~(S//NF)~~

In Section I, we provide a brief overview of the National Security Agency (NSA) and the inception of the Stellar Wind program, including a description of the legal authorities relied upon to support the program and the scope of collection authorized under the Presidential Authorizations. In Section II, we describe key aspects of the NSA's implementation of the Presidential Authorizations, [redacted] the technical operation of the program, and the initial process for analyzing and disseminating the information collected. In Sections III and IV, we describe the FBI's and the Office of Intelligence Policy and Review's early knowledge of and involvement in Stellar Wind. In Section V, we describe measures the FBI implemented to improve its management of information derived from the program that the FBI disseminated to its field offices. ~~(TS//STLW//SI//OC/NF)~~

I. Inception of the Stellar Wind Program (U//~~FOUO~~)

A. The National Security Agency (U)

The NSA was established on October 24, 1952, by President Truman as a separate agency within the Department of Defense under the direction, authority, and control of the Secretary of Defense. See Presidential Memorandum to the Secretary of State and the Secretary of Defense, October 24, 1952. By Executive Order 12333 (December 4, 1981), the NSA was given responsibility within the U.S. Intelligence Community for all signals intelligence, including the "collection of signals intelligence for national foreign intelligence purposes" and the processing and dissemination of such intelligence for counterintelligence purposes.[19] (U)

---

[19] Signals intelligence is defined as:

1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. (U)

2. Intelligence derived from communications, electronic, and foreign instrumentation signals. (U)

(Cont'd.)

The NSA's two primary missions are to protect U.S. government information systems and to collect, process, and disseminate foreign signals intelligence information. This twofold mission is reflected in the NSA's organizational structure, which consists of two operational directorates: The Information Assurance Directorate, which conducts defensive information operations to protect information infrastructures critical to the United States' national security interests, and the Signals Intelligence Directorate (SID), which controls foreign intelligence collection and processing activities for the United States. (U)

The SID is divided into three major components, two of which – Analysis and Production [redacted] and Data Acquisition [redacted] – are relevant to the Stellar Wind program. The work of these components with respect to the Stellar Wind program is discussed in more detail in Section II below. ~~(S//NF)~~

B. Implementation of the Program (September 2001 through November 2001) ~~(S//NF)~~

Immediately following the September 11 terrorist attacks, the NSA modified how it conducted some of its traditional signals collection activities. [redacted] ~~(TS//SI//NF)~~

George Tenet, the Director of Central Intelligence at the time, mentioned the modification of these NSA collection activities during a meeting with Vice President Cheney shortly after the September 11 attacks to discuss the intelligence community's response. According to Hayden, who did not attend the meeting but was told about it by Tenet, Cheney asked Tenet to inquire from the NSA whether there were additional steps that could be taken with respect to enhancing signals intelligence capabilities. Tenet related this message to Hayden, who responded that there was nothing further the NSA could do without additional authority. According to Hayden, Tenet asked him a short time later what the NSA could do if additional authority was provided. ~~(TS//SI//NF)~~

Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 484. (U)

Hayden consulted with experts from the NSA's SID and attorneys from the NSA's Office of General Counsel about how the NSA could enhance its collection capabilities consistent with considerations of operational usefulness, technical feasibility, and legality. Hayden said he then attended a meeting at the White House to discuss how NSA signals intelligence collection capabilities could be modified to respond to the September 11 attacks. ~~(TS//SI//NF)~~

Hayden told us he highlighted two issues at this meeting. First, Hayden stated at the meeting that the FISA statute's applicability to evolving telecommunications technology had the effect of constraining the NSA's ability to intercept communications [redacted] According to Hayden, the NSA was authorized under Executive Order 12333 to [redacted] Thus, the NSA could not direct its traditional foreign intelligence collection activities [redacted] without having to first obtain FISA Court authorization.[21] ~~(TS//SI//NF)~~

The second issue Hayden highlighted at the meeting concerned the meta data associated with telephonic and e-mail communications. Hayden said that obtaining access to the meta data of communications to and from

---

[20] The FISA statute defines "wire communication" as "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." 50 U.S.C. § 1801(l). By its terms, FISA governs the acquisition of wire communications to or from persons in the United States if such acquisition occurs in the United States. See 50 U.S.C. § 1801(f)(2). [redacted] (U)

[21] [redacted]

the United States, as well as communications within the United States, would significantly enhance the NSA's analytical capabilities. ~~(TS//SI//NF)~~

Hayden said he attended two additional meetings with Vice President Cheney to discuss further how NSA collection capabilities could be expanded along the lines described at the White House meeting. Vice President Cheney directed Hayden to meet with the Counsel to the Vice President, David Addington, to continue the discussion, which Hayden said he did. According to Hayden, Addington drafted the first Presidential Authorization for the Stellar Wind program based on these meetings.[22] ~~(TS//STLW//SI//OC/NF)~~

The Stellar Wind program officially came into existence on October 4, 2001, when President Bush signed the Presidential Authorization drafted by Addington. The Authorization directed the Secretary of Defense to employ the signals intelligence capabilities of the NSA to collect certain foreign intelligence by electronic surveillance in order to prevent acts of terrorism within the United States.[23] The Presidential Authorization stated that an extraordinary emergency existed because of the September 11 attacks, constituting an urgent and compelling governmental interest permitting electronic surveillance within the United States for counterterrorism purposes without judicial warrants or court orders. ~~(TS//STLW//SI//OC/NF)~~

Access to the Stellar Wind program was very tightly restricted. Former White House Counsel and Attorney General Alberto Gonzales told the OIG that it was the President's decision to keep the program a "close hold." Gonzales stated that the President made the decision on all requests to read in non-operational persons, including Justice Department officials, and that as far as he was aware this decision-making authority had not been delegated either within the White House or to other agencies concerning read-in decisions for operational personnel, such as NSA and

---

[22] Hayden told us he could not recall the Justice Department having any involvement in or presence at meetings he attended to discuss enhancing NSA collection capabilities. Hayden said this mildly surprised him but that he assumed someone was keeping the Department briefed on these discussions. Gonzales, who was the White House Counsel at the time, also told the OIG that he would be "shocked" if the Department was not represented at the White House meetings, and further stated that in the immediate aftermath of September 11, he met often with lawyers from the NSA, CIA, DOD, and the Justice Department with the objective of "coordinating the legal thinking" concerning the United States' response to the attacks. Because we were unable to interview Addington, former Attorney General Ashcroft, and John Yoo, we do not know what role if any the Department played in drafting or reviewing the first Presidential Authorization. ~~(TS//SI//NF)~~

[23] The program was given the cover term [redacted] at which time the cover term was changed to "Stellar Wind." ~~(S//NF)~~

FBI employees.[24] However, as indicated in the NSA Office of the Inspector General's report on the President's Surveillance Program (NSA OIG Report), decisions to read in NSA, CIA, and FBI operational personnel were made by the NSA. According to the NSA OIG Report, NSA Director Hayden needed White House approval to read in members of Congress, FISA Court judges, the NSA Inspector General, and others. See NSA OIG Report at V. ~~(S//NF)~~

1. Pre-Stellar Wind Office of Legal Counsel Legal Memoranda (U)

In this section, we summarize the initial legal memoranda from the Justice Department supporting the legal basis for the Stellar Wind program, and we describe the key aspects of the first Presidential Authorization for the program. ~~(TS//STLW//SI//OC/NF)~~

a. Hiring of John Yoo (U)

OLC Deputy Assistant Attorney General John Yoo was responsible for drafting the first series of legal memoranda supporting the program.[25] As noted above, Yoo was the only OLC official "read into" the Stellar Wind program from the program's inception until he left the Department in May 2003.[26] The only other non-FBI Department officials read into the program until after Yoo's departure were Attorney General Ashcroft, who was read in on October 4, 2001, and Counsel for Intelligence Policy James Baker, who was read in on January 11, 2002.[27] ~~(TS//STLW//SI//OC/NF)~~

---

[24] Gonzales testified before the Senate Judiciary Committee on July 18, 2006, that "[a]s with all decisions that are non-operational in terms of who has access to the program, the President of the United States makes the decisions, because this is such an important program[.]" (U)

[25] The Office of Legal Counsel typically drafts memoranda for the Attorney General and the Counsel to the President, usually on matters involving significant legal issues or constitutional questions, and in response to legal questions raised by Executive Branch agencies. In addition, all Executive Orders proposed to be issued by the President are reviewed by the Office of Legal Counsel as to form and legality, as are other matters that require the President's formal approval. (U)

[26] The process of being "read into" a compartmented program generally entails being approved for access to particularly sensitive and restricted information about a classified program, receiving a briefing about the program, and formally acknowledging the briefing, usually by signing a nondisclosure agreement describing restrictions on the handling and use of information concerning the program. (U)

[27] Daniel Levin, who served as both Chief of Staff to FBI Director Robert Mueller and briefly as Ashcroft's national security counselor, also was read into the program along with Mueller in late September 2001 at the FBI. According to Levin, White House Counsel Gonzales controlled who was read into the program, but Gonzales told him that the President had to personally approve each request. ~~(TS//STLW//SI//OC/NF)~~

Jay Bybee, the Assistant Attorney General for the Office of Legal Counsel from November 2001 through March 2003, provided the OIG with background information on how Yoo came to be involved in national security issues on behalf of the OLC. Bybee's nomination to be the OLC Assistant Attorney General was announced by the White House in July 2001. Bybee was not confirmed by the Senate as the Assistant Attorney General until late October 2001.[28] For several weeks after the September 11, 2001, terrorist attacks, Bybee remained a law professor at the University of Nevada-Las Vegas, and was sworn in as OLC Assistant Attorney General in late November 2001. ~~(TS//SI//NF)~~

Bybee told us that he traveled to Washington, D.C., sometime in July 2001 to interview applicants for Deputy Assistant Attorney General slots in OLC. In early July 2001, Kyle Sampson, at the time a Special Assistant to the President and Associate Director for Presidential Personnel assigned to handle presidential appointments to the Department of Justice, told Bybee that John Yoo was already under consideration for one of the OLC Deputy Assistant Attorney General slots. Bybee said Sampson asked him whether he would agree to have Yoo be one of his deputies. Bybee said that he knew Yoo only by reputation but was "enthusiastic" about the prospect of having Yoo as a Deputy. Bybee told the OIG that he regarded Yoo as a "distinguished hire." Bybee said that after speaking with Sampson he called Yoo and asked him to work at OLC as a Deputy Assistant Attorney General. (U)

In addition to speaking with Yoo, Bybee interviewed other prospective OLC Deputies, and hired several individuals, including Patrick Philbin and Ed Whelan, for those positions.[29] The White House recommended, and Bybee agreed, that Whelan be designated Principal Deputy. Bybee stated that he knew Yoo would be disappointed because Yoo had wanted that position, and Bybee said that Yoo "didn't hide his disappointment." Bybee told us that Yoo asked him whether since he was not selected for the Principal Deputy slot he could be guaranteed the "national security portfolio." Bybee agreed to Yoo's request. Bybee told the OIG that this was an easy decision because Yoo had more national security experience than any of the other deputies. (U)

---

[28] Bybee told us that Daniel Koffsky was the Acting Assistant Attorney General at this time. (U)

[29] Bybee told us that all Deputy candidates were also interviewed by the White House. As described in Chapter Four of this report, Philbin played a central role in the Department's reassessment of the legal basis for the Stellar Wind program after John Yoo left the Department in May 2003. ~~(TS//SI//NF)~~

Bybee said that Yoo began working in OLC in July 2001 and that all of the Deputies were in place before Bybee began serving as head of the OLC that November. (U)

Bybee told us he was never read into the Stellar Wind program and could shed no further light on how Yoo came to draft the OLC opinions on the program. However, he said that Yoo had responsibility for supervising the drafting of opinions related to national security issues by the time the attacks of September 11 occurred.[30] Bybee described Yoo as "articulate and brilliant," and also said he had a "golden resume" and was "very well connected" with officials in the White House. He said that from these connections, in addition to Yoo's scholarship in the area of executive authority during wartime, it was not surprising that Yoo "became the White House's guy" on national security matters. (U)

b. Yoo's Legal Analysis of a Warrantless Domestic Electronic Surveillance Program ~~(TS//SI//NF)~~

Before the start of the Stellar Wind program under the October 4, 2001, Presidential Authorization, Yoo drafted a memorandum evaluating the legality of a "hypothetical" electronic surveillance program within the United States to monitor communications of potential terrorists. His memorandum, dated September 17, 2001, was addressed to Timothy Flanigan, Deputy White House Counsel, and was entitled "Constitutional Standards on Random Electronic Surveillance for Counter-Terrorism Purposes." ~~(TS//STLW//SI//OC/NF)~~

Yoo drafted a more extensive version of this memorandum, dated October 4, 2001, for White House Counsel Gonzales. [redacted] (U//FOUO)

[redacted] ~~(TS//SI//NF)~~

---

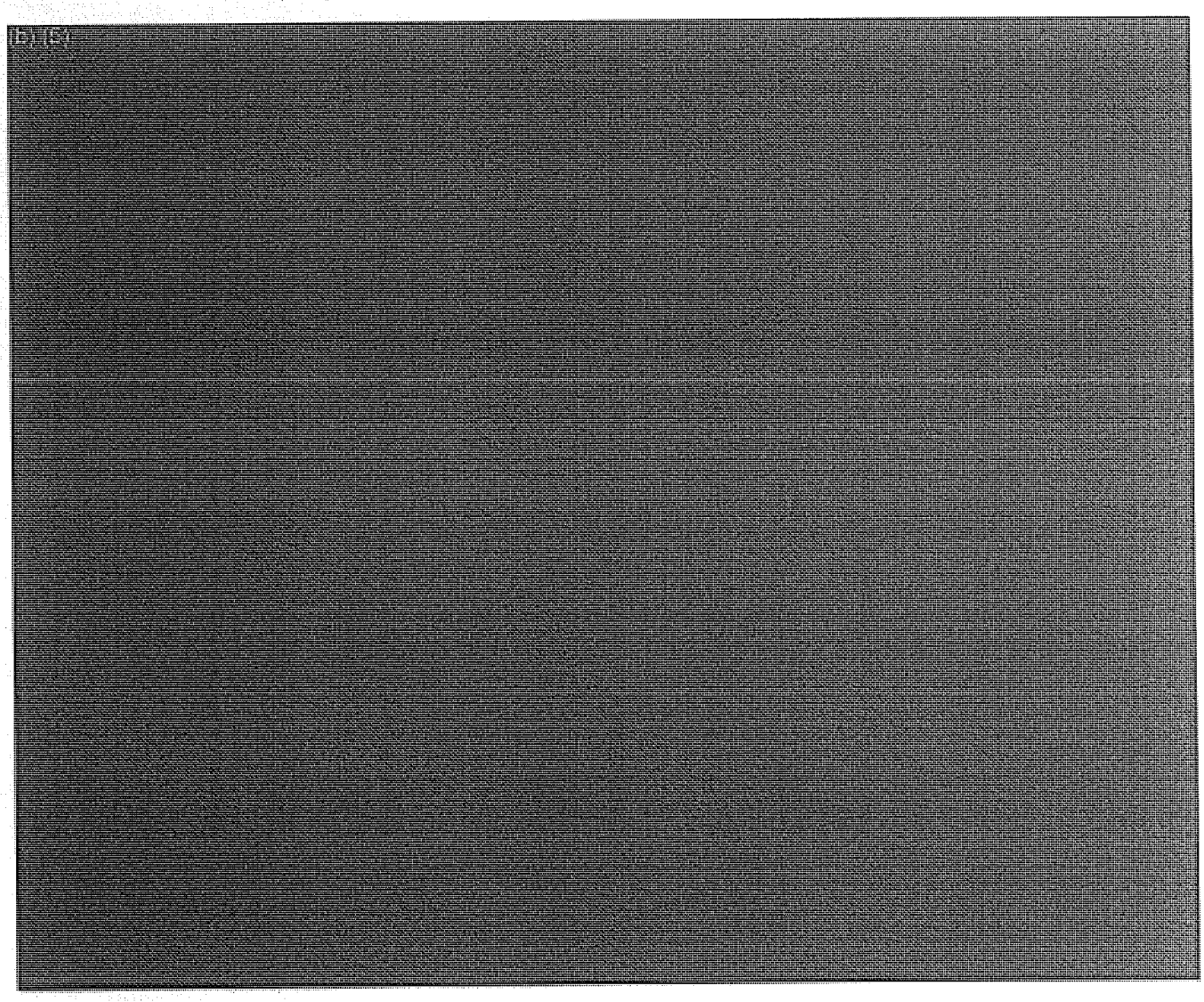
[30] As noted above, Yoo, Ashcroft, Card, and Addington declined or did not respond to our request for interviews, and we do not know how Yoo came to deal directly with the White House on legal issues surrounding the Stellar Wind program. In his book "War by Other Means," Yoo wrote that "[a]s a deputy to the assistant attorney general in charge of the office, I was a Bush Administration appointee who shared its general constitutional philosophy. . . . I had been hired specifically to supervise OLC's work on [foreign affairs and national security]." John Yoo, *War by Other Means*, (Atlantic Monthly Press, 2006), 19-20. ~~(TS//SI//NF)~~

[redacted]

[redacted]

[redacted]

(b) (5)



[redacted][33] is an example of how the October 4 memorandum did not reflect the Stellar Wind program as it was actually devised and operated by the NSA. The Stellar Wind program did not contemplate bulk collection of content communications. The only information collected in bulk under the program involved telephony and e-mail meta data. This meta data was collected in bulk so that it could then be queried based on telephone numbers or e-mail addresses associated with communicants with known or suspected links to international terrorism. These telephone numbers and e-mail addresses are known as "selectors." ~~(TS//STLW//SI/OC/NF)~~

(b) (5)

Yoo's September 17 and October 4 memoranda were not addressed specifically to the Stellar Wind program, but rather to a "hypothetical" randomized or broadly scoped domestic warrantless surveillance program. As discussed below, the first Office of Legal Counsel opinion explicitly addressing the legality of the Stellar Wind program was not drafted until after the program had been formally authorized by President Bush on October 4, 2001. ~~(TS//SI//OC/NF)~~

Gonzales told the OIG that he did not believe these first two memoranda fully addressed the White House's understanding of the Stellar Wind program. Rather, as described above, these memoranda addressed the legality of a "hypothetical" domestic surveillance program rather than the Stellar Wind program as authorized by the President and carried out by the NSA.[35] However, Gonzales also told us that he believed these first two memoranda described as lawful activities that were broader than those carried out under Stellar Wind, and that therefore these opinions "covered" the Stellar Wind program. ~~(TS//SI//NF)~~

2. Presidential Authorization of October 4, 2001 ~~(TS//SI//NF)~~

On October 4, 2001, President Bush issued the first of 43 Presidential Authorizations for the Stellar Wind program. The October 4 Authorization directed the Secretary of Defense to "use the capabilities of the Department of Defense, including but not limited to the signals intelligence capabilities of the National Security Agency, to collect foreign intelligence by electronic surveillance," provided the surveillance was intended to:

> (a) acquire a communication (including but not limited to a wire communication carried into or out of the United States by cable) for which there is probable cause to believe that [redacted] (b)(1), (b)(3) a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or an agent of such a group; or
>
> (b) acquire, with respect to a communication, header/router/addressing-type information, including telecommunications dialing-type data, but not the contents of the communication, when (i) at least one party to such communication is outside the United States or (ii) no party to such communication is known to be a citizen of the United States. ~~(TS//STLW//SI//OC/NF)~~

---

[35] Gonzales noted that Deputy White House Counsel Timothy Flanigan, the recipient of the first Yoo memorandum, was not read into Stellar Wind. (U//~~FOUO~~)

In short, this first Authorization allowed NSA to intercept the content of any communication, including those to, from, or exclusively within the United States, where probable cause existed to believe one of the communicants was engaged in international terrorism, (b)(1), (b)(3) [redacted] The Authorization also allowed the NSA to "acquire" telephony and e-mail meta data where one end of the communication was foreign or neither communicant was known to be a U.S. citizen.[36] ~~(TS//STLW//SI//OC/NF)~~

The Authorization stated that it relied primarily on Article II of the Constitution and on the recently passed Authorization for the Use of Military Force (AUMF) to support the intelligence-gathering activities. The Authorization also stated that the President's directive was based on threat assessments indicating that terrorist groups remained determined to attack in the United States. The Authorization stated that it was to terminate "not later than 30 days" from the date of its execution.
~~(TS//STLW//SI//OC/NF)~~

As several Office of Legal Counsel and other Department and NSA officials acknowledged, in addition to allowing the interception of the content of communications into or out of the United States, the literal terms of paragraph 4(a)(ii) of this first Authorization would have allowed NSA to intercept the content of purely domestic communications. NSA Director Hayden told us he did not realize this until Addington specifically raised the subject during a meeting the two had to discuss renewing the first Authorization. According to Hayden, he told Addington that he did not want the NSA conducting such domestic interceptions and cited three reasons for this. First, he said the NSA was a *foreign* intelligence agency. Second, the NSA's collection infrastructure would not support the collection of purely domestic communications. Third, Hayden said he would require such a high evidentiary standard to justify intercepting purely domestic communication that such cases might just as well go to the FISA Court.[37]
~~(TS//STLW//SI//OC/NF)~~

[redacted]
(b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~

[37] Hayden said Addington did not pressure him on the subject and simply modified the next Authorization to provide that the NSA may only intercept the content of communications that originated or terminated in the United States. We discuss the modifications to the Authorization in the next part of this chapter.
~~(TS//STLW//SI//OC/NF)~~

As a result, Hayden said the NSA did not exercise the apparent authority in the first Authorization to intercept domestic-to-domestic communications. Goldsmith stated that Hayden's position that the NSA not involve itself in domestic spying related back to NSA's "getting in a lot of trouble" for its abuses during the 1970s. In addition, former Deputy Attorney General Comey told us that Hayden had said he was willing to "walk up to the line" but would be careful "not to get chalk on [his] shoes." ~~(TS//STLW//SI//OC/NF)~~

As discussed above, subsection (b) of paragraph 4 of the Authorization covered the acquisition of both e-mail and telephony meta data. The e-mail meta data included the "to," "from," "cc," "bcc," and "sent" lines of an e-mail, but not the "subject" line or content of the e-mail. (b)(1), (b)(3) [redacted] Telephony meta data acquisition included the dialing information from telephone billing data, such as the originating and terminating telephone number and the date, time, and duration of the telephone calls, but not the content of telephone calls. Under the Presidential Authorization, collection of both e-mail and telephony meta data was limited to circumstances in which one party to the communication was outside the United States or no party to the communication was known to be a U.S. citizen. ~~(TS//STLW//SI//OC/NF)~~

Attorney General Ashcroft approved the first Presidential Authorization as to "form and legality" on October 4, 2001. According to NSA records, this was the same day that Ashcroft was verbally read into the Stellar Wind program. Daniel Levin, who in October 2001 was both a national security counselor to Attorney General Ashcroft and FBI Director Mueller's Chief of Staff, told us that, according to Ashcroft, the Presidential Authorization was "pushed in front of" Ashcroft and he was told to sign it.[38] Levin stated that he was not with Ashcroft when this occurred and therefore he did not have an opportunity to advise Ashcroft about the Authorization before Ashcroft signed it. ~~(TS//STLW//SI//OC/NF)~~

James Baker, Counsel for Intelligence Policy, told us that Levin had given him the same account of how Ashcroft came to approve the October 4, 2001, Presidential Authorization. According to Baker, Ashcroft was told that the program was "critically important" and that it must be approved as to form and legality. Baker said that Levin told him Ashcroft approved the

[38] According to Hayden, Addington typed the Presidential Authorizations and personally couriered them around for signatures. However, the OIG was unable to determine whether Addington presented the first Authorization to Ashcroft for signature, because both Ashcroft and Addington declined or did not respond to our requests to interview them. ~~(S//NF)~~

Authorization on the spot. According to Baker, Levin also told Baker that when he learned there was no memorandum from the Office of Legal Counsel concerning the program, Levin told Yoo to draft one. ~~(TS//STLW//SI//OC/NF)~~

Levin's account to us of the instruction that Yoo draft a memorandum concerning the legality of the program differed slightly from Baker's account. Levin told us that he said to Ashcroft that it "wasn't fair" that Ashcroft was the only Justice official read into the program, and that for Ashcroft's protection Levin advised Ashcroft to have another Department official read into the program for the purpose of providing advice on the legality of the program. Levin said he learned that Ashcroft was able to get permission from the White House to have one other person read into the program to advise Ashcroft, although Levin was not certain how Yoo came to be selected as that person.[39] As discussed below, Gonzales told us that it was the President's decision to read John Yoo into the program. ~~(TS//STLW//SI//OC/NF)~~

C. Presidential Authorization is Revised and the Office of Legal Counsel Issues Legal Memoranda in Support of the Program (November 2001 through January 2002) ~~(TS//STLW//SI//OC/NF)~~

1. Presidential Authorization of November 2, 2001 ~~(TS//SI//NF)~~

On November 2, 2001, with the first Presidential Authorization set to expire, President Bush signed a second Presidential Authorization. The second Authorization relied upon the same authorities in support of the President's actions, chiefly the Article II Commander-in-Chief powers and the AUMF. The second Authorization cited the same findings in a threat assessment as to the magnitude of the potential threats and the likelihood of their occurrence in the future. However, the scope of authorized content collection and meta data acquisition was redefined by adding the italicized language below in paragraphs 4(a) and (b):

> (a) acquire a communication (including but not limited to a wire communication carried into or out of the United States by cable) for which, *based on the factual and practical considerations of everyday life there are reasonable grounds* to believe that [redacted]

[39] By October 4, 2001, Yoo had already drafted two legal analyses on a hypothetical warrantless surveillance program and therefore already had done some work related to the program prior to October 4 when Ashcroft was read in. ~~(TS//SI//NF)~~

(b)(1), (b)(3) [redacted] *such communication originated or terminated outside the United States and* a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or *any* agent of such a group; or

(b) acquire, with respect to a communication, header/router/addressing-type information, including telecommunications dialing-type data, but not the contents of the communication, when (i) at least one party to such communication is outside the United States, (ii) no party to such communication is known to be a citizen of the United States, *or (iii) based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are specific and articulable facts giving reason to believe that such communication relates to international terrorism, or activities in preparation therefor.* ~~(TS//STLW//SI//OC/NF)~~

The new language therefore changed in three key respects the scope of collection and acquisition authorized under the Stellar Wind program. First, the "probable cause to believe" standard for the collection of e-mail and telephone content was replaced with "for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe . . . ." Baker told us this change was made by Addington because he believed the term "probable cause" was "too freighted" with usage in judicial opinions. Baker said he believed the change to more colloquial language also was made because the standard was to be applied by non-lawyers at the NSA. ~~(TS//STLW//SI//OC/NF)~~

Second, the new standard applied to the reasonable belief that "such communication originated or terminated outside the United States . . . ." The new language therefore eliminated the authority that existed in the first Authorization to intercept the content of purely domestic communications. ~~(TS//STLW//SI//OC/NF)~~

Third, the second Authorization permitted the acquisition of a third category of e-mail and telephony meta data when "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are specific and articulable facts giving reason to believe that such communication relates to international terrorism, or activities in preparation therefore." This language represented an expansion of meta data collection authority to include meta data pertaining to certain communications even when both parties are U.S. persons, as long as there were facts giving reason to believe that the communication was related to international terrorism. ~~(TS//STLW//SI//OC/NF)~~

In addition, former OLC Principal Deputy and Acting Assistant Attorney General Steven Bradbury described this [redacted] (b) (5) [redacted] ~~(TS//STLW//SI//OC/NF)~~

2. Yoo Drafts Office of Legal Counsel Memorandum Addressing Legality of Stellar Wind ~~(TS//STLW//SI//OC/NF)~~

The Stellar Wind program was first authorized by President Bush and certified as to form and legality by Attorney General Ashcroft on October 4, 2001, without the support of any formal legal opinion from the Office of Legal Counsel expressly addressing Stellar Wind. ~~(TS//SI//NF)~~

The first OLC opinion directly supporting the legality of the Stellar Wind program was dated November 2, 2001, and was drafted by Yoo. His opinion also analyzed the legality of the first Presidential Authorization and a draft version of the second Authorization.[40] ~~(TS//SI//NF)~~

In his November 2 memorandum to Attorney General Ashcroft, Yoo opined that the Stellar Wind program [redacted] (b) (5) [redacted] As discussed in Chapter Four of this report, however, perceived deficiencies in Yoo's memorandum later became critical to the Office of Legal Counsel's decision to reassess the Stellar Wind program in 2003. We therefore describe Yoo's legal analysis in his November 2 memorandum. ~~(TS//SI//NF)~~

Yoo acknowledged at the outset of his November 2 memorandum that "[b]ecause of the highly sensitive nature of this subject and the time pressures involved, this memorandum has not undergone the usual editing and review process for opinions that issue from our Office [OLC]." The memorandum then reviewed the changes to NSA's collection authority between the first and second Presidential Authorizations. [redacted] (b) (5) [redacted]

[40] The second Authorization was issued on November 2, 2001. In developing his legal memorandum, Yoo analyzed a draft of the second Authorization dated October 31, 2001. The OIG was not provided the October 31 draft Presidential Authorization, but based on Yoo's description in his November 2 memorandum, it appears that the draft that Yoo analyzed tracked the language of the final November 2, 2001, Authorization signed by the President. ~~(TS//SI//NF)~~

[redacted]

~~(TS//STLW//SI//OC/NF)~~

[redacted]

Yoo did acknowledge in his memorandum that the first Presidential Authorization was "in tension with FISA." Yoo stated that FISA "purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence," but Yoo then opined that "[s]uch a reading of FISA would be an unconstitutional infringement on the President's Article II authorities."[41] Citing advice of the OLC and the position of the Department as presented to Congress during passage of the USA PATRIOT Act several weeks earlier, Yoo characterized FISA as merely providing a "safe harbor for electronic surveillance," adding that it "cannot restrict the President's ability to engage in warrantless searches that protect the national security." ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[41] As discussed in Chapter Four, Goldsmith criticized this statement as conclusory and unsupported by any separation of powers analysis. (U//~~FOUO~~)

Regarding whether the activities conducted under the Stellar Wind program could be conducted under FISA, Yoo wrote that it was problematic that FISA required an application to the FISA Court to describe the (b)(1), (b)(3) or "facilities" to be used by the target of the surveillance. Yoo also stated that it was unlikely that a FISA Court would grant a warrant to cover (b)(1), (b)(3) as contemplated in the Presidential Authorization. Noting that the Authorization could be viewed as a violation of FISA's civil and criminal sanctions in 50 U.S.C. §§ 1809-10, Yoo opined that in this regard FISA represented an unconstitutional infringement on the President's Article II powers. According to Yoo, the ultimate test of whether the government may engage in warrantless electronic surveillance activities is whether such conduct is consistent with the Fourth Amendment, not whether it meets the standards of FISA. ~~(TS//STLW//SI//OC/NF)~~

Citing cases applying the doctrine of constitutional avoidance, Yoo reasoned that reading FISA to restrict the President's inherent authority to conduct foreign intelligence surveillance would raise grave constitutional questions.[42] Yoo wrote that "unless Congress made a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless searches in the national security area – which it has not – then the statute must be construed to avoid such a reading."[43] ~~(TS//STLW//SI//OC/NF)~~

---

[42] Yoo's memorandum cited the doctrine of constitutional avoidance, which holds that "where an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress." *Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Construction Trades Council*, 485 U.S. 568, 575 (1988). Yoo cited cases supporting the application of this doctrine in a manner that preserves the President's "inherent constitutional power, so as to avoid potential constitutional problems." See, e.g., *Public Citizen v, Department of Justice*, 491 U.S. 440, 466 (1989). ~~(TS//STLW//SI//OC/NF)~~

[43] On March 2, 2009, the Justice Department released nine opinions written by the OLC from 2001 through 2003 regarding "the allocation of authorities between the President and Congress in matters of war and national security" containing certain propositions that no longer reflect the views of the OLC and "should not be treated as authoritative for any purpose." Steven G. Bradbury, Principal Deputy Assistant Attorney General, Office of Legal Counsel, Department of Justice, Memorandum for the Files, "Re: Status of Certain OLC Opinions Issued in the Aftermath of the Terrorist Attacks of September 11, 2001," January 15, 2009, 1, 11. Among these opinions was a February 2002 classified memorandum written by Yoo which asserted that Congress had not included a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless surveillance activities in the national security area and that the FISA statute therefore does not apply to the president's exercise of his Commander-in-Chief authority. In a January 15, 2009, memorandum (included among those released in March), Bradbury stated that this proposition "is problematic and questionable, given FISA's express references to the President's authority" and is "not supported by convincing reasoning." ~~(TS/STLW//SI//OC/NF)~~

Yoo's analysis of this point would later raise serious concerns for other officials in the Office of Legal Counsel and the Office of the Deputy Attorney General (ODAG) in late 2003 and early 2004.[44] Among other concerns, Yoo did not address the 15-day warrant requirement exception in FISA following a congressional declaration of war. See 50 U.S.C. § 1811. Yoo's successors in the Office of Legal Counsel criticized this omission in Yoo's memorandum because they believed that by including this provision in FISA, Congress arguably had demonstrated an intention to "occupy the field" on the matter of electronic surveillance during wartime.[45] ~~(TS//STLW//SI//OC/NF)~~

Yoo's memorandum next analyzed Fourth Amendment issues raised by the Presidential Authorizations. Yoo dismissed Fourth Amendment concerns regarding the NSA surveillance program to the extent that the Authorizations applied to non-U.S. persons outside the United States. Regarding those aspects of the program that involved interception of the international communications of U.S. persons in the United States, Yoo asserted that Fourth Amendment jurisprudence allowed for searches of persons crossing the border and that interceptions of communications in or out of the United States fell within the "border crossing exception." Yoo further opined that electronic surveillance in "direct support of military operations" did not trigger constitutional rights against illegal searches and seizures, in part because the Fourth Amendment is primarily aimed at curbing law enforcement abuses. ~~(TS//STLW//SI//OC/NF)~~

Finally, Yoo wrote that the electronic surveillance described in the Presidential Authorizations was "reasonable" under the Fourth Amendment and therefore did not require a warrant. In support of this position, Yoo cited Supreme Court opinions upholding warrantless searches in a variety of contexts, such as drug testing of employees and sobriety checkpoints to detect drunk drivers, and in other circumstances "when special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable," *Veronia School Dist. 47J v. Acton*, 515 U.S. 464, 652 (1995) (as quoted in November 2, 2001, Memorandum at 20). Yoo wrote that in these situations the government's interest was found to have outweighed the individual's privacy interest, and that in this regard "no governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 435 U.S. 280, 307 (1981). According

---

[44] One of these officials was Patrick Philbin, who following Yoo's departure was "dual-hatted" as both an Associate Deputy Attorney General and a Deputy Assistant Attorney General in the Office of Legal Counsel. (U)

[45] We discuss the OLC's reassessment and criticism of Yoo's analysis in Chapter Four. (U)

to Yoo, the surveillance authorized by the Presidential Authorizations advanced this governmental security interest. ~~(TS//STLW//SI//OC/NF)~~

Yoo's memorandum focused almost exclusively on content interceptions.

(b)(5)

~~(TS//STLW//SI//OC/NF)~~

(b)(5); (b)(1); (b)(3)

Yoo also omitted from his November 2 memorandum – as well as from his earlier September 17 and October 4, 2001, memoranda – any discussion of *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), a leading case on the distribution of government powers between the Executive and

[44]

(b)(5); (b)(1); (b)(3)

Legislative branches.[47] As discussed in Chapter Four, Justice Jackson's analysis of President Truman's Article II Commander-in-Chief authority during wartime in the *Youngstown* case was an important factor in the Office of Legal Counsel's reevaluation in 2004 of Yoo's opinion on the legality of the Stellar Wind program. ~~(TS//SI//NF)~~

3. Additional Presidential Authorizations (U)

On November 30, 2001, the President signed a third Authorization authorizing the Stellar Wind program. The third Authorization was virtually identical to the second Authorization of November 2, 2001, in finding that the threat of terrorist attacks in the United States continued to exist, the legal authorities cited for continuing the electronic surveillance, and the scope of collection. ~~(TS//STLW//SI//OC/NF)~~

OLC Principal Deputy and Acting Assistant Attorney General Bradbury told the OIG that [redacted] (b)(1), (b)(3) Accordingly, the fourth Presidential Authorization, signed on January 9, 2002, modified the scope of collection to provide:

> (a) acquire a communication (including but not limited to a wire communication carried into or out of the United States by cable) for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe such communication originated or terminated outside the United States and a party to such communication is a group

---

[47] In *Youngstown*, the Supreme Court held that President Truman's Executive Order directing the Secretary of Commerce to seize and operate steel plants during a labor dispute to produce steel needed for American troops during the Korean War was an unconstitutional exercise of the President's Article II Commander-in-Chief authority. In a concurring opinion, Justice Jackson listed three categories of Presidential actions against which to judge the Presidential powers. First, "[w]hen the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum[.]" Id. at 635. Second, Justice Jackson described a category of concurrent authority between the President and Congress as a "zone of twilight" in which the distribution of power is uncertain and dependant on "the imperatives of events and contemporary imponderables rather than on abstract theories of law." Id. at 637 (footnote omitted). Third, "[w]hen the President takes measures incompatible with the express or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter." Id. Justice Jackson concluded that President Truman's actions fell within this third category, and thus "under circumstances which leave Presidential power most vulnerable to attack and in the least favorable of possible constitutional postures." Id. at 640. (U)

engaged in international terrorism, or activities in preparation therefor, or any agent of such a group; or

(b) acquire, with respect to a communication, header/router/addressing-type information, including telecommunications dialing-type data, but not the contents of the communication, when (i) at least one party to such communication is outside the United States, (ii) no party to such communication is known to be a citizen of the United States, or (iii) based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are specific and articulable facts giving reason to believe that such communication relates to international terrorism, or activities in preparation therefor.

Presidential Authorization, January 9, 2002. (~~TS//STLW//SI//OC/NF~~)

(b)(1), (b)(3) [redacted] The language of the Authorization as modified in January 2002 remained the collection standard in subsequent Presidential Authorizations extending the Stellar Wind Program, until the disputed Presidential Authorization in March 2004, which we discuss in Chapter Four. (~~TS//STLW//SI//OC/NF~~)

4. Subsequent Yoo Opinions (U)

In a 2-page memorandum to Attorney General Ashcroft dated January 9, 2002, Yoo wrote that (b)(1), (b)(3), (b) (5) [redacted] did not affect the legality of the Authorization. (~~TS//STLW//SI//OC/NF~~)

Several identical Presidential Authorizations recertifying the Stellar Wind program were signed in 2002. (U//~~FOUO~~)

In October 2002, at Attorney General Ashcroft's request, Yoo drafted another opinion for Ashcroft concerning the Stellar Wind program. This memorandum, dated October 11, 2002, reiterated the same basic analysis in Yoo's November 2, 2001, memorandum in support of the legality of the Stellar Wind program.[48]

(b) (5) [redacted]

[48] As in the November 2, 2001, memorandum, Yoo's October 11, 2002, memorandum included the following caveat: "Because of the highly sensitive nature of this subject and its level of classification, this memorandum has not undergone the usual editing and review process for opinions that issue from our Office [OLC]." (~~TS//STLW//SI//OC/NF~~)

(b)(5)

~~(TS//STLW//SI//OC/NF)~~

(b)(5)

5. Yoo's Communications with the White House (U)

As the only Office of Legal Counsel official who had been read into the Stellar Wind program through early 2003, Yoo consulted directly with White House officials about the program during this period. Because we were unable to interview Yoo, we could not determine the exact nature and extent of these consultations. We were also unable to determine whether Ashcroft was fully aware of the advice Yoo was providing directly to the White House about the program. ~~(S//NF)~~

Gonzales told the OIG that Yoo was among those with whom the White House consulted to develop advice for the President on the program, but he asserted that Yoo was not sought out to provide approval of the program for the Department. However, Gonzales told us that he did not know how Yoo came to be the primary Justice Department official that the White House consulted during this period about the program. ~~(S//NF)~~

In fact, Jay Bybee, who served as the OLC Assistant Attorney General for most of this period and was Yoo's supervisor, was never read into the Stellar Wind program. Bybee told the OIG that during his tenure as Assistant Attorney General he did not know that Yoo was working alone on a sensitive compartmented program and he had no knowledge of how Yoo

came to be selected for this responsibility. Bybee told us that he was "surprised" and "a little disappointed" to learn in media accounts that he was not privy to Yoo's work on what Bybee had later learned to be a compartmented counterterrorism program involving warrantless electronic surveillance. Bybee said that it would not be unusual for a Deputy Assistant Attorney General such as Yoo to have direct contact with the White House for the purpose of rendering legal advice, but that the OLC Assistant Attorney General must be aware of all opinions that issue from the OLC. Bybee said that the Assistant Attorney General has an obligation to "see the whole picture" and is the person in the office who knows the full range of issues that are being addressed by the OLC and who can assure that OLC opinions remain consistent. ~~(TS//SI//NF)~~

6. Gonzales's View of the Department's Role in Authorizing the Stellar Wind Program ~~(S//NF)~~

The OIG asked Gonzales about how he, as White House Counsel, viewed the role of the Justice Department during the early phase of the Stellar Wind program. Gonzales stated that he and others at the White House tried to be very careful to understand what could be done legally, and they wanted to have "constant communications with the Department" in the first few months following the September 11, 2001, terrorist attacks. Gonzales also stated that it was the President, and not the Attorney General or the White House Counsel, who authorized the warrantless surveillance activity under the Stellar Wind program. However, Gonzales acknowledged that the President's decision was based on advice from the Attorney General and White House Counsel, among others. ~~(TS//SI//NF)~~

The OIG also asked whether Gonzales had a personal belief about the justification for having a single attorney – Yoo – speak on behalf of the Department regarding the legality of the program. Gonzales stated that it was up to the Attorney General to make that determination or calculation. Gonzales stated that he understood the Department's position was that the program was legal and that Yoo would sit down with Attorney General Ashcroft to answer any legal questions when the Presidential Authorizations were presented to Ashcroft for his signature. Gonzales said he understood that the Yoo opinions represented the legal opinion of the Department. However, as noted previously, for the first year and a half of the program the Department read-ins included only Yoo, Ashcroft, and Baker. ~~(TS//SI//NF)~~

Gonzales also stated that it was Ashcroft's decision as to how to satisfy his legal obligations as Attorney General. However, when the OIG asked whether Gonzales was aware if Ashcroft ever requested to have additional people read into Stellar Wind, Gonzales stated that he recalled Ashcroft wanted Deputy Attorney General Larry Thompson and his Chief of Staff, David Ayres, read in. Gonzales acknowledged that neither official was

ever read into the program. Gonzales said that Ashcroft complained that it was "inconvenient" not to have Thompson and Ayres read in, but Gonzales also stated that he never got the sense from Ashcroft that it affected the quality of the legal advice the Department provided to the White House. Gonzales stated that other than Ashcroft's request that Thompson and Ayres be read in, he did not recall Ashcroft requesting to have additional Department officials read in.[49] ~~(S//NF)~~

II. NSA's Implementation of the Stellar Wind Program (U//~~FOUO~~)

In this section, we describe the NSA's initial implementation of the Stellar Wind program. We first describe how the NSA acquired the communications data authorized for collection under the program. We also discuss the process the NSA used to analyze the information received from the Stellar Wind program and how this information was provided to the FBI. (U//~~FOUO~~)

A. Implementation of Stellar Wind (U//~~FOUO~~)

Our description of the implementation of the Stellar Wind program is based on NSA and Justice Department documents we obtained during our review, as well as interviews of NSA and Department personnel with knowledge of Stellar Wind's technical operation. This section provides a basic overview of how the NSA obtained (b)(1), (b)(3) the information authorized for collection under Stellar Wind. This information is also important for later sections of this report that describe significant modifications to the Authorizations regarding the manner and scope of collection, the Department's re-assessment of the legal rationale supporting the Stellar Wind program during late 2003 and early 2004, and compliance issues that arose when the Department decided to seek collection of (b)(1), (b)(3)

(TS//STLW//SI//OC/NF)

(b)(1), (b)(3)

[49] Gonzales stated that Ashcroft, as the Attorney General, would be well-positioned to request the President to allow additional attorneys to be read into the program. Drawing on his own experience as Attorney General, Gonzales cited his request to the President in 2006 that the then head of the Office of Professional Responsibility (OPR) and several attorneys within OPR be granted security clearances in order to conduct an inquiry into the professional conduct of Department lawyers with respect to the Stellar Wind program. Gonzales said he made his request both through White House Counsel Harriet Miers and directly to the President. However, the President initially declined the request, and the request was not granted until October 2007. (U//~~FOUO~~)

[redacted] As discussed previously, the NSA collected three categories of information under Stellar Wind that came to be commonly referred to as the three "baskets." Basket 1 referred to collection of the content of telephone and e-mail communications; basket 2 referred to collection of meta data associated with telephone communications; and basket 3 referred to collection of meta data associated with e-mail and other Internet communications. [redacted][52] ~~(TS//STLW//SI//OC/NF)~~

[50] [redacted]

[51] We describe in Chapter Four changes made in March and [redacted] 2004 [redacted] under Presidential Authorization following a dispute between the White House and Justice Department concerning the legality of the Stellar Wind program. [redacted] ~~(TS//SI//NF)~~

[52] Title 18 of the United States Code generally prohibits the interception and disclosure of wire, oral, or electronic communications, and provides for criminal penalties for any person engaging in such activity. See 18 U.S.C. § 2511. [redacted]

The meta data collected [redacted] under Stellar Wind (baskets 2 and 3), as well as the meta data associated with communications targeted for content collection under the program, was placed into an NSA database system called [redacted] which according to NSA officials is a configuration of databases and analytical tools. [redacted] databases are segregated into "realms" organized by the specific authority allowing the particular data to be collected.[53] The content data collected under the Stellar Wind program was placed in a separate NSA repository.[54] ~~(TS//STLW//SI//OC/NF)~~

1. Basket 1 – Telephone and E-Mail Content Collection ~~(TS//STLW//SI//OC/NF)~~

a. Telephone Communications (U)

In this section we describe briefly the technical means used by the NSA to access the international telephone system to accomplish the collection of international calls under the Stellar Wind program.[55] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

(U)

[redacted]

[53] NSA officials said the realms also establish a system of access control to ensure that only authorized users access certain data. ~~(S//NF)~~

[54] As discussed in Chapter Five of this report, the NSA created an additional realm in July 2004 when the government obtained FISA authority to collect e-mail meta data, and another realm in May 2006 when it obtained authority under FISA to collect telephony meta data. These realms were separate from the realms that contained information collected under Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

[55] The NSA's interception of international telephone communications under Stellar Wind highlighted the dramatic change in telecommunications technology that had been taking place for nearly 20 years. In 1978, when FISA was enacted, telephone calls placed by and to individuals within the United States (domestic calls) were carried mostly on copper wires, while telephone calls placed to or from individuals outside the United States (international calls) generally were transmitted by satellites. FISA reflected the state of technology then by defining the term "electronic surveillance" to be the acquisition of the contents of certain wire and radio (satellite) communications. FISA stated that as to radio

(Cont'd.)

[redacted]

communications specifically, and thus as to most international communications, the interception of calls constituted "electronic surveillance" only if the acquisition intentionally targeted a particular known U.S. person in the United States, or if all participants to the communication were located in the United States. See 50 U.S.C. §§ 1801(f)(1) and (3). Accordingly, government surveillance that targeted foreign persons outside the United States generally was not considered electronic surveillance under FISA, and the government was not required to obtain a FISA Court order authorizing the surveillance even if one of the parties to the communication was in the United States.

~~(TS//STLW//SI//OC/NF)~~

[redacted]

[redacted]

b. E-Mail Communications (TS//SI//NF)

[redacted]

[redacted]

[redacted] However, under the October 4, 2001, Presidential Authorization, the NSA for the first time was authorized to intercept international e-mails originating or terminating inside the United States. [redacted]

[redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[redacted]

[redacted]

[redacted]

2. Basket 2 – Telephony Meta Data Collection
~~(TS//STLW//SI//OC/NF)~~

[redacted]

[redacted]

The NSA informed the FISA Court of this issue in the government's December 2006 FISA application that sought to bring Stellar Wind's content collection under FISA authority (discussed in Chapter Five of this report).

[redacted]

~~(TS//STLW//SI//OC/NF)~~

[redacted] These records, also referred to as call detail records, consist of routing information that includes the originating and terminating telephone number of each call, and the date, time, and duration of each call. The call detail records do not include the substantive content of any communication or the name, address, or financial information of a subscriber or customer. ~~(TS//STLW//SI//OC/NF)~~

As discussed above, the initial Presidential Authorizations [redacted] that is, call detail records pertaining to communications where at least one party was outside the United States, where no party was known to be a United States citizen, or where there was reasonable articulable suspicion to believe the communication related to international terrorism. As noted in Chapter One, the NSA interpreted this authority to also permit it to collect telephony and e-mail meta data in bulk so that it would have a database from which to acquire the targeted meta data. [redacted] (TS//STLW//SI//OC/NF)

[redacted]

[redacted]

[redacted]

(Cont'd.)

[redacted]

[redacted] The NSA personnel also organized the data into a format that could be used by NSA analysts responsible for analyzing the information under the Stellar Wind program. The data was archived into an NSA analytical database that contained exclusively Stellar Wind information and that was accessible only by specially authorized NSA personnel read into the program. ~~(TS//STLW//SI//OC/NF)~~

[redacted] [63] While the magnitude of the bulk collection was enormous, the NSA did not retrieve or review most of this data because access was authorized only with respect to telephone communications that satisfied the Presidential Authorizations "acquisition" standard. In fact, the NSA reported that by the end of 2006, .001% of the data collected had actually been retrieved from its database for analysis. ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[63] We describe these techniques in part B of this section. (U)

3. Basket 3 – E-Mail Meta Data Collection

~~(TS//STLW//SI//OC/NF)~~

[redacted]

The meta data the NSA obtained from e-mail communications included the information that appeared on the "to," "from," "cc," "bcc," and "sent" lines of a standard e-mail. Thus, the NSA collected the e-mail address of the sender, the e-mail addresses of any recipients, and the information concerning the date and time when the e-mail was sent.

~~(TS//STLW//SI//OC/NF)~~

[redacted] The meta data collection did not include information from the "subject" or "re" lines of the e-mails or the body of the e-mails.[64]

~~(TS//STLW//SI//OC/NF)~~

[redacted]

[64] [redacted]

[redacted] ~~(TS//STLW//SI//OC/NF)~~

B. NSA Process for Analyzing Information Collected Under Stellar Wind ~~(S//NF)~~

The NSA conducted two functionally distinct types of review of the massive amount of data it collected under the Stellar Wind program. First, the NSA conducted procedures intended to ensure that it only reviewed or "acquired" the information that was within the scope of the Presidential Authorizations. Second, the NSA conducted substantive analysis of the acquired information to determine whether it had intelligence value that should be disseminated to customer agencies such as the FBI and the CIA. ~~(TS//SI//NF)~~

The NSA procedures to ensure that the acquisition and dissemination standards were satisfied became more formalized over time. We describe below how the NSA handled the enormous volume of data it was collecting with the Stellar Wind program. ~~(TS//SI//NF)~~

1. Basket 1: Content tasking, Analysis, and Dissemination ~~(TS//STLW//SI//OC/NF)~~

Stellar Wind's "basket 1" content database contains telephone and e-mail communications of individuals. The NSA refers to the telephone numbers and e-mail addresses tasked for interception as "selectors." To task a selector under the Presidential Authorizations, the NSA was required to establish probable cause to believe the intercepted communications originated or terminated outside the United States and probable cause to believe a party to the communications was a group engaged in international terrorism, or activities in preparation therefor, or any agent of such a group.[65] ~~(TS//STLW//SI//OC/NF)~~

The NSA had two processes for tasking selectors under Stellar Wind. One process applied to tasking foreign selectors, or selectors believed to be

[redacted]

used by non-U.S. persons outside the United States. The other process applied to tasking domestic selectors, or selectors believed to be used by persons inside the United States or by U.S. persons abroad. A foreign selector could be tasked for collection under Stellar Wind based upon an NSA analyst's determination, following some amount of documented research and analysis about the selector, that the terms of the Authorizations were satisfied. The NSA did not require any additional levels of approval before a foreign selector could be tasked.[66]
~~(TS//STLW//SI//OC/NF)~~

A domestic selector could be tasked only after the NSA analyst obtained specific approvals. The rigor of the process to task a domestic selector evolved over time, but essentially it required an analyst to draft a formal tasking package that demonstrated, through analysis and documentation, that the selector satisfied the terms of the Authorizations. This package was reviewed by a designated senior official who could approve or reject the package, or request that additional information be provided.
~~(TS//STLW//SI//OC/NF)~~

In emergency situations, the NSA could commence content interception on a selector within [redacted] of identifying a number or address that satisfied the criteria in the Presidential Authorizations. In other cases, interception commenced within [redacted] for urgent or priority taskings and within a week for routine taskings. ~~(TS//STLW//SI//OC/NF)~~

The NSA conducted 15-, 30-, and 90-day reviews of tasked foreign and domestic selectors to assess whether the interception should continue. The NSA stated that the selectors were "de-tasked" if the user was arrested, if probable cause could no longer be established, or if other targets took priority. ~~(TS//STLW//SI//OC/NF)~~

The content intercepted under taskings was sent to the NSA and placed in a database accessible by NSA analysts cleared into the Stellar Wind program. The analysts were responsible for reviewing the communications and assessing whether a Stellar Wind report should be generated for the FBI and the CIA. [redacted]

[redacted]

[redacted]

~~(TS//STLW//SI//OC/NF)~~

2. Baskets 2 and 3: Telephony and E-Mail Meta Data Queries, Analysis, and Dissemination ~~(TS//STLW//SI//OC/NF)~~

The NSA received [redacted] a massive amount of telephony and e-mail meta data (basket 2 and 3 information) that was stored in a realm accessible only by NSA analysts assigned to the Stellar Wind program. The purpose of the collection was to facilitate the identification of connections [redacted] among particular telephone numbers and e-mail addresses by using [redacted] sophisticated analytical techniques called "contact chaining" [redacted] ~~(TS//STLW//SI//OC/NF)~~

As described by the NSA in declarations filed with the FISA Court, contact chaining is used to determine the contacts made by a particular telephone number or e-mail address (tier one contacts), as well as contacts made by subsequent contacts (tier two and tier three contacts). The NSA uses computer algorithms to identify the first two tiers of contacts an e-mail address makes and the first three tiers of contacts a telephone number makes. According to the NSA, multi-tiered contact analysis is particularly useful with telephony meta data because a telephone does not lend itself to simultaneous contact with large numbers of individuals as e-mail does with spam.

[redacted]

~~(TS//STLW//SI//OC/NF)~~

[redacted]

As previously noted, the NSA interpreted the Presidential Authorizations to permit it to collect telephony and e-mail meta data in bulk.[67] The NSA "queried" the databases that held this data to identify meta data for communications to or from a particular telephone or e-mail address (the "selector," also known as the "seed number" or "seed account"). NSA analysts queried the database using a selector for which there was a reasonable articulable suspicion to believe that the number or account had been used for communications related to international terrorism.[68]

~~(TS//STLW//SI//OC/NF)~~

As with proposals to task selectors, an NSA shift coordinator typically reviewed for approval proposals to query either the e-mail or telephony meta data bulk databases using particular selectors. If the shift coordinator agreed that the reasonable articulable suspicion standard was met, the selector was approved and the analyst was authorized to query the meta data bulk database to identify all of the other telephone numbers or e-mail addresses that had been in contact with the seed account. Each contact along the chain of contacts that originated with the selector was referred to as a "hop," meaning that a telephone call from the seed account to telephone number A was considered "one hop out," and a call from telephone number A to telephone number B was considered "two hops out" (relative to the seed account), and so on. NSA analysts used specialized software to chain and analyze the contacts identified by each query. The

[67]

[68]

NSA told us that Stellar Wind analysts were permitted to chain the results of queries up to three hops out from the selector. ~~(TS//STLW//SI//OC/NF)~~

The results of each query were analyzed to determine whether any of the contacts should be reported, or "tipped," to Stellar Wind customers – primarily the FBI, CIA, and the National Counterterrorism Center. In the first months of the Stellar Wind program, the NSA reported to the FBI most contacts identified between a U.S. telephone number or e-mail address and the selector used to query the meta data realm, as well as domestic contacts that were two and three hops out from a selector. As discussed in Chapter Six of this report, over time the NSA and FBI worked to improve the reporting process and the quality of the intelligence being disseminated under Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

The domestic contacts from specified numbers or e-mail addresses, called "tippers," were provided to the FBI by the NSA. These tippers were included in reports that contained two sections separated by a dashed line, commonly referred to as a "tearline," made to appear as a perforation extending across the width of a page. The purpose of the tearline was to separate the compartmented information above the tearline, which could identify the specific sources and methods used to obtain the information, from the non-compartmented information that the FBI could further disseminate to its field offices. Only FBI personnel read into the Stellar Wind program could have access to the full Stellar Wind reports from NSA. ~~(TS//STLW//SI//OC/NF)~~

The information that appeared above the tearline typically was classified Top Secret/SCI and identified Stellar Wind as the source of the intelligence. The information included specific details [redacted] as well as any pertinent comments by NSA intelligence analysts. ~~(TS//STLW//SI//OC/NF)~~

The information that appeared below the tearline of a report generally was classified Secret or Confidential and did not identify Stellar Wind as the source of the intelligence. The text typically included some version of the following statement:

[redacted]

The amount of information about the contacts that followed this statement varied. [redacted]

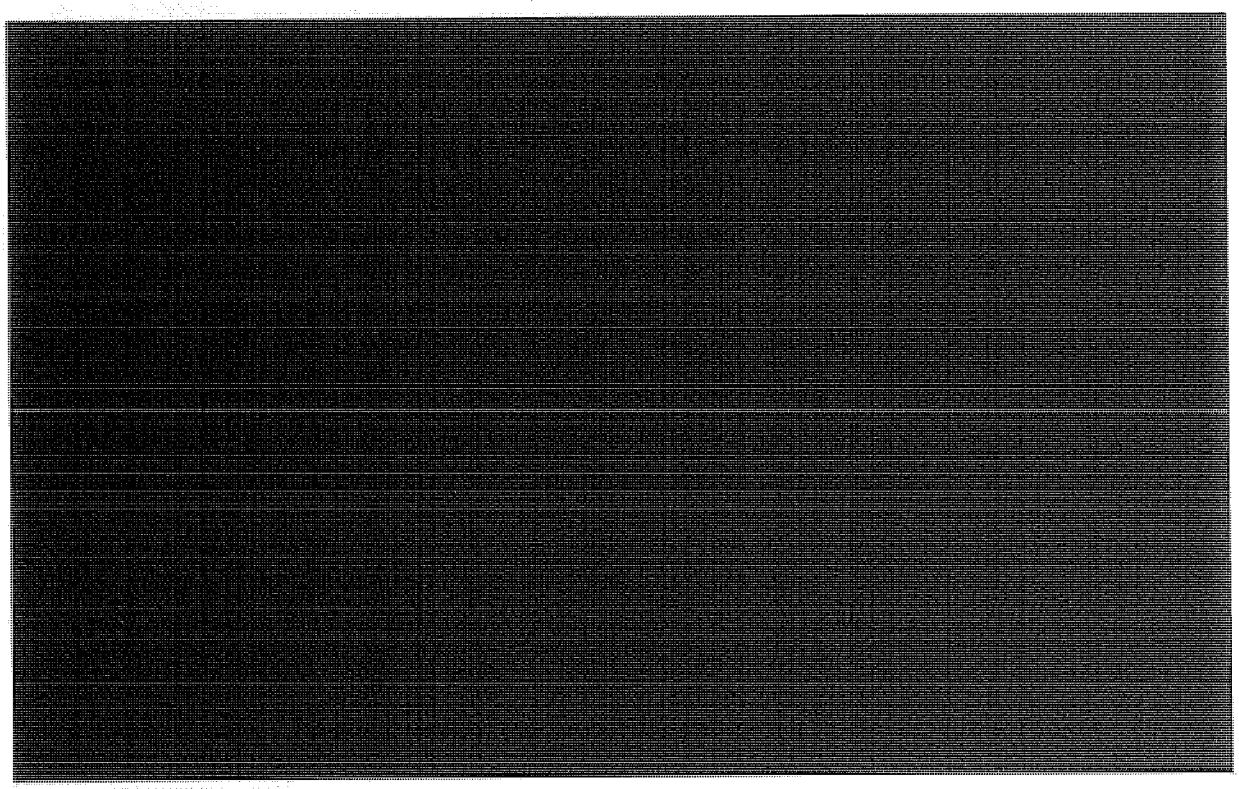
[redacted] and provided the date or dates of the contacts, or the period of time in which contact was made. ~~(TS//STLW//SI//OC/NF)~~

During the first several months of the Stellar Wind program, nearly all reports based on telephone or e-mail meta data analysis designated each of the tippers as [redacted]

~~(TS//STLW//SI//OC/NF)~~

As examples, the following Stellar Wind reports were among those disseminated to the FBI in November 2001. We have excerpted only the information below the tearline, which is often referred to simply as "tearline information." In addition, we did not provide the actual telephone numbers provided by the NSA to the FBI. ~~(TS//SI//NF)~~

[redacted]



b1,
b3,
b7E

III. FBI's Early Participation in the Stellar Wind Program ~~(S//NF)~~

Stellar Wind was not an FBI program, nor was the FBI involved in the program's creation. However, as the lead agency for counterterrorism in the United States, the FBI received much intelligence produced under Stellar Wind. In the following sections, we describe how the FBI became involved in the Stellar Wind program, the personnel resources allocated to handle Stellar Wind information, and the initial procedures the FBI established to receive, control, and disseminate the program information. ~~(TS//STLW//SI//OC/NF)~~

---

[69] In addition to the queries the NSA conducted on a case-by-case basis, the NSA also maintained a list of foreign and domestic telephone numbers and e-mail addresses for which, based on NSA analysts' assessments, there was a reasonable basis to believe were associated with international terrorism. These selectors, called "alerts," were queried against the incoming meta data automatically on a daily basis, and any contacts with a domestic telephone number or e-mail address were directed to NSA analysts for review and possible reporting to the FBI. The NSA regularly updated the alert list by adding or removing selectors, depending on the available intelligence. As we discuss in Chapter Five in connection with the transition of Stellar Wind's bulk meta data collection from presidential authority to FISA authority, the FISA Court found that the NSA's use of the alert list to query incoming telephone meta data did not comply with terms of the Court's Order. ~~(TS//STLW//SI//OC/NF)~~

A. FBI Director First Informed of Stellar Wind Program (U//~~FOUO~~)

Director Mueller told us that his earliest recollection of the Stellar Wind program was a meeting he attended at the White House with Attorney General Ashcroft, which occurred either after the decision had been made to move forward with the presidentially authorized program or shortly after the October 4, 2001, Authorization was issued. Mueller told us the meeting was "more than a formal read-in" and that Director Hayden may have attended. Mueller said that at or around this time he also briefly reviewed the October 4, 2001, Presidential Authorization, which he characterized as "relatively complex." ~~(TS//SI//OC/NF)~~

Director Mueller said his impression at the time was that the terms of the Presidential Authorization might allow for collecting purely domestic telephone and e-mail communications. Mueller said he discussed the matter with Ashcroft and asked whether OLC had issued an opinion on the program. Mueller said that he recalled being told that OLC might have opined orally on the program and Mueller said he suggested to Ashcroft that OLC issue a formal written opinion. Mueller told us that he did not think the NSA ever exercised authority under the Authorization to collect purely domestic communications. ~~(TS//STLW//SI//OC/NF)~~

Mueller stated that based on the meeting he attended at the White House and his brief review of the October 4, 2001, Presidential Authorization, he understood the FBI's role in the Stellar Wind program was to be a "recipient" of intelligence generated by the NSA, and to provide any technical support to the NSA as necessary to support the program. ~~(TS//SI//NF)~~

B. [redacted]

[redacted]

b1, b3, b7E

[redacted]

[70] Executive Order 12333 authorizes the FBI to provide operational support to the Intelligence Community. (U)

[71] [redacted]

b1, b3, b7E

[redacted]

b1,
b3,
b7E

[redacted]

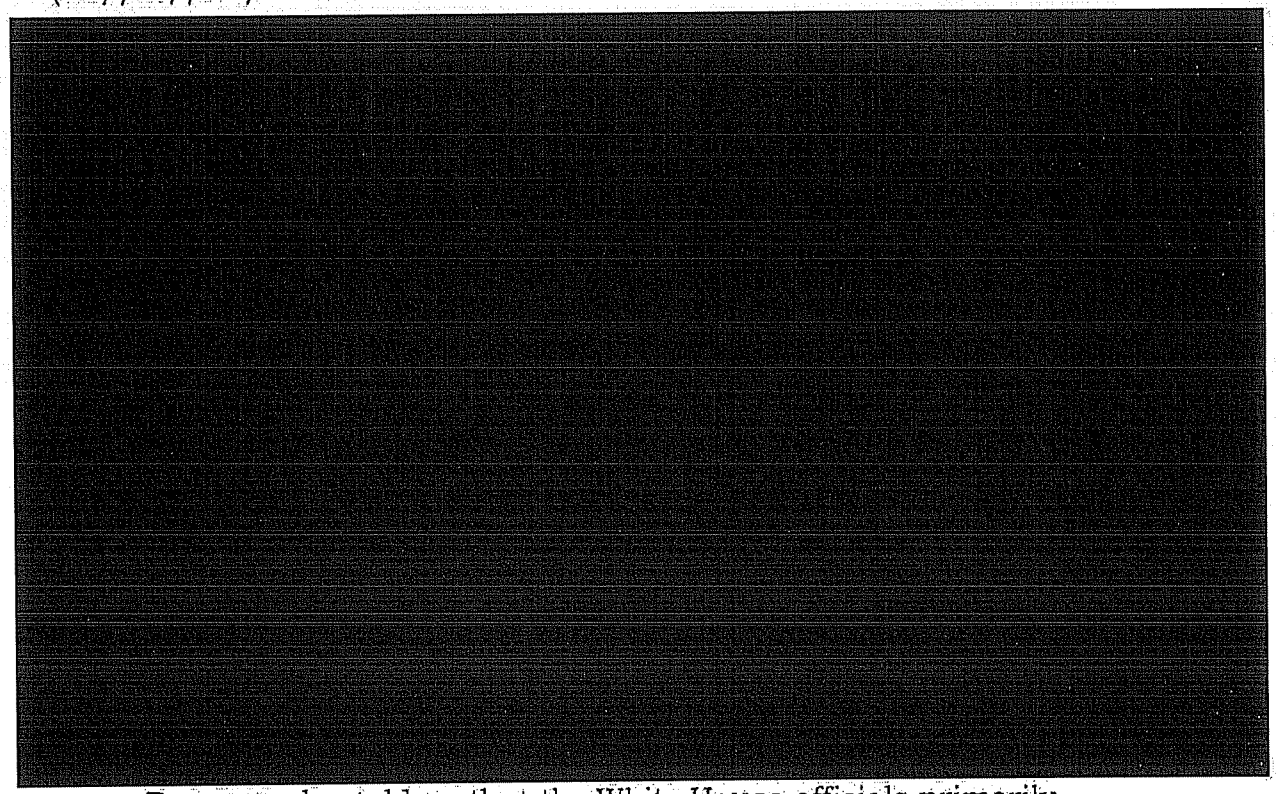
Mueller said he therefore decided to request an order from the

Attorney General formally directing the FBI to support the NSA program. Mueller said that he also requested the order because he wanted a "record as to our participation." ~~(TS//STLW//SI//OC/NF)~~

In response, on October 20, 2001, Attorney General Ashcroft sent a memorandum to Director Mueller stating:

> As part of the Nation's self defense activities, the National Security Agency (NSA) is engaged in certain additional collection activities, the details of which you are aware. Those activities are legal and have been appropriately authorized, and the Federal Bureau of Investigation should cooperate with NSA as necessary for it to conduct those activities. ~~(TS//SI//NF)~~

According to Mueller, the combination of this memorandum from the Attorney General and the November 2, 2001, memorandum prepared by the Department's Office of Legal Counsel regarding the legality of Stellar Wind gave him comfort at that time with the FBI's participation in the program. ~~(TS//SI//NF)~~



Bowman also told us that the White House officials primarily responsible for Stellar Wind, who he identified as the Vice President and Addington, were "amateurs" when it came to intelligence work. Bowman stated that one of the potential consequences of severely limiting the number of individuals read into a program is that uncleared personnel who

occupy positions placing them in close proximity to program-related activities might construe certain actions as questionable or illegal and report that activity, thereby potentially compromising the activities. Bowman said that this is what occurred with Stellar Wind. For this reason and others, Bowman did not agree with the decision to so severely limit access to the program. ~~(TS//STLW//SI//OC/NF)~~

[redacted]

C. FBI Begins to Receive and Disseminate Stellar Wind "Tippers" ~~(S//NF)~~

In the immediate aftermath of the September 11 terrorist attacks, the FBI had created a task force of agents and analysts to analyze the flood of telephone numbers it received from multiple sources, including agencies within the U.S. Intelligence Community, foreign intelligence services, and concerned citizens. The task force, called the Telephone Analysis Unit (TAU), was located at FBI Headquarters and consisted of approximately 50 FBI employees working on shift rotations 24 hours per day, 6 days per week. The operation was supervised by FBI supervisors working out of the FBI's Strategic Information and Operations Center. As described below, personnel assigned to this task force were among the first at the FBI to handle Stellar Wind-derived information. ~~(TS//STLW//SI//OC/NF)~~

1. FBI Initiates [redacted] ~~(S//NF)~~ b1, b3, b7E

In October or November 2001, several TAU analysts were assigned to what came to be called the [redacted] which was the FBI's effort to manage the Stellar Wind-derived information being received from the NSA. The information, referred to as Stellar Wind "tippers," consisted of telephone numbers and e-mail accounts derived from NSA meta data analysis, and sometimes content intercepted from particular telephone and e-mail communications. The essential purpose of the [redacted] was to receive Stellar Wind tippers from the NSA and disseminate the information to FBI field offices for investigation in a manner that did not reveal the source of the information or the methods by which it was collected. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

Working alternating shifts in the FBI's Strategic Information and Operations Center, two FBI analysts were primarily responsible for managing Stellar Wind tippers in the initial months of the program. These analysts told the OIG that until December 2001, the Stellar Wind tippers

consisted nearly exclusively of telephone numbers. According to the analysts, the process for handling Stellar Wind tippers began when the NSA liaison co-located at FBI Headquarters provided one of the analysts the information below the tearline from a Stellar Wind report containing one or more tippers. The analyst then queried FBI databases for any information about each tipper, such as whether the tipper appeared in any pending or closed FBI investigations. The analyst also queried the tipper against the FBI's [redacted] database, which is the FBI's central repository for telephone subscriber data acquired during the course of investigations. In addition, the analyst checked each tipper against public source databases for relevant information, such as the identity of a telephone number subscriber. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

After completing these database checks, the analyst drafted an Electronic Communication, or EC, from FBI Headquarters to the appropriate FBI field office. The EC described the tearline information about the tipper contained in the Stellar Wind report together with any additional information the analyst was able to locate. ~~(TS//STLW//SI//OC/NF)~~

The [redacted] ECs disseminated to field offices included several features concerning the nature of the information and how it could be used. First, the ECs advised the field offices that the information being provided was "derived from an established and reliable source" and that it was "being addressed by the TAU as the [redacted]"[72] ~~(S//NF)~~ b1, b3, b7E

Second, the ECs included a caveat about the use of the information being provided, stating that the information "is for lead purposes only and is intended solely for the background information of recipients in developing their own collateral leads. It cannot be used in affidavits, court proceedings, subpoenas, or for other legal or judicial purposes." The FBI said this language was included in each EC to protect the source of the information and the methods by which it was collected. ~~(S//NF)~~

Third, the ECs provided an explanation about the qualitative rankings assigned to the tippers. As described previously, the NSA assigned each tipper a [redacted] ranking [redacted][73] ~~(TS//SI//NF)~~

[redacted] ~~(S//NF)~~ b1, b3, b7D, b7E

(Cont'd.)

Fourth, the ECs instructed the field offices how the tippers should be addressed. These instructions were provided as "leads," for which the FBI had three categories: Action, Discretionary, and For Information. An Action lead instructed a field office to take a particular action in response to the EC. An Action lead was "covered" when the field office took the specified action or conducted appropriate investigation to address the information in the EC. A Discretionary lead allowed the field office to take whatever action it deemed appropriate. A field office that receives a "For Information" lead was not expected to take any specific action in response to the EC other than possibly route the communication to the office personnel whose investigations or duties the information concerned. ~~(S//NF)~~

After the FBI analyst completed this process and drafted the EC, an FBI Supervisory Special Agent read into the Stellar Wind program reviewed the EC, in part to ensure that it did not reveal the source of the information or the method by which the information was obtained. Once approved, the analyst entered the EC into the FBI's Automated Case Management System and the receiving field offices were notified electronically to review the communication. ~~(TS//SI//NF)~~

Each [redacted] EC typically contained multiple tippers and therefore was distributed to multiple field offices. The receiving field offices were responsible for handling the leads that concerned tippers falling in their respective geographic jurisdictions. ~~(S//NF)~~ b1, b3, b7E

Most of the [redacted] leads that disseminated Stellar Wind tippers were designated Action leads. As noted, during this period the tippers were almost exclusively telephone numbers. Accordingly, the typical lead instructed the field office to [redacted] The lead also instructed the field office to report the investigative results to the Telephone Analysis Unit. ~~(TS//SI//NF)~~ b1, b3, b7E

The two [redacted] analysts told us that the focus of their work in the first months after the September 11 attacks was to detect what many believed was an imminent second attack. During this period, nearly all of the Stellar Wind tippers the FBI received were disseminated to a field office for investigation as quickly as possible. ~~(S//NF)~~ b1, b3, b7E

In addition to tippers containing the content of intercepted telephone and e-mail communications (content tippers), in approximately December

[redacted] ~~(TS//SI//NF)~~

2001 the NSA began providing the FBI tippers derived from the NSA's e-mail meta data analysis (e-mail tippers). These e-mail tippers initially were routed to the same two analysts who were managing the telephone tippers. The analysts told us that the e-mail tippers were processed and disseminated in the same manner as the telephone tippers. Content tippers, which according to the analysts were received very infrequently during this early period, generally were also disseminated by EC to the appropriate field offices, but little if any research regarding the information was conducted. The analysts said they considered the content tippers particularly time-sensitive and for that reason occasionally transmitted the ECs directly to the appropriate field offices or called the offices to advise that the information was being loaded into the FBI's Automated Case Management System. In 2002, responsibility for e-mail tippers was reassigned to the Electronic Communications Analysis Unit.
~~(TS//STLW//SI//OC/NF)~~

In February 2002, one of the two FBI analysts left the [redacted] after being selected for a management position in a different analytical section within the FBI's Counterterrorism Division. The remaining analyst became solely responsible for managing the Stellar Wind tippers under the [redacted] a situation that continued for approximately the next 12 months. The analyst told us that while her work hours during this period were "ridiculous," she did not feel there was any pressure to add analysts to the project because "the process was working well." ~~(TS//SI//NF)~~ b1, b3, b7E

In early 2002, FBI management instructed the lone [redacted] analyst to conduct some of her work while physically located in the NSA Headquarters at Fort Meade, Maryland. This created an unusual arrangement for the analyst. The analyst continued to receive the NSA's daily Stellar Wind reports at FBI Headquarters, and she would then drive to the NSA with the reports to draft the ECs (the analyst had remote access to FBI databases from an NSA workstation). The analyst told us that interaction with NSA counterparts during these daily visits was minimal. After the ECs were drafted, the analyst returned to FBI Headquarters to obtain approval to disseminate the communications to the FBI's field offices. The analyst's impression was that FBI management created this unusual arrangement "for show" and that its purpose was to establish an FBI "presence" at the NSA in connection with Stellar Wind. b1, b3, b7E
~~(TS//STLW//SI//OC/NF)~~

The analyst continued working on Stellar Wind matters until approximately February 2003, when a small team of FBI personnel were

assigned permanently to the NSA to manage the FBI's participation in the Stellar Wind program.[74] ~~(S//NF)~~

2. FBI Field Offices' Response to [redacted] Leads ~~(S//NF)~~

b1, b3, b7E

According to the two FBI analysts responsible for managing Stellar Wind information under the [redacted] from approximately October 2001 to February 2003, some agents in FBI field offices grew frustrated with the information they were receiving under the program. Because the [redacted] ECs that disseminated the tippers to the field offices assigned most of them as Action leads, this required that the leads be covered expeditiously. ~~(S//NF)~~

b1, b3, b7E

Under ordinary operating procedures, investigative leads for international terrorism matters are set by FBI Headquarters' International Terrorism Operations Section. In addition, the ECs assigning international terrorism leads typically identified a Supervisory Special Agent within ITOS as the point-of-contact for any questions field offices might have. Because the Stellar Wind program was so tightly compartmented, the leads sent during this early period by the [redacted] were not coordinated with ITOS, and the FBI Headquarters point-of-contact identified in the ECs for any questions generally was one of the two [redacted] analysts. ~~(S//NF)~~

b1, b3, b7E

According to one of the [redacted] analysts, agents responsible for covering the Action leads complained that the lack of background information provided in the ECs about the tippers made it difficult to determine what investigative steps could or should be taken. [redacted][75] Consequently, the analyst

b1, b3, b7E

[74] This co-location of FBI personnel at the NSA is discussed below. ~~(S//NF)~~

[75] To open a full investigation, the FBI was required to [redacted] A preliminary inquiry required only a showing of [redacted] See Attorney General Guidelines for [redacted] The FBI's practice of issuing national security letters based on Stellar Wind-derived information is discussed in Chapter Six of this report. ~~(S//NF)~~

b1, b3, b7E

received calls from agents requesting additional information about the source of the intelligence provided in the ECs to help the agents decide whether there was sufficient predication to open an investigation on the telephone number or to issue a national security letter for subscriber information. ~~(TS//SI//NF)~~

The analyst stated that in response to these calls he could only reiterate to the agents that the information was provided by a reliable, sensitive source. The analyst said this situation produced a "dichotomy" with the tippers. On the one hand, there was a demand in the International Terrorism Operations Section and field offices for the telephone numbers because of their priority [redacted] status and the prevailing concern that there would be a second terrorist attack; on the other hand, the limited and vague information contained in the [redacted] ECs caused some confusion and frustration among agents investigating the lead. ~~(S//NF)~~ b1, b3, b7E

Agents also complained that many tippers were already known to the FBI from past or pending investigations and that the [redacted] ECs were providing "circular reporting."[76] However, according to one [redacted] analyst, this generally did not occur. The analyst explained that an agent in the field assigned to cover a lead on a telephone number did not know the NSA was the source of the intelligence. Consequently, when the agent discovered that the number was identical to a number the agent was already investigating or was aware of, it appeared to the agent that the [redacted] simply had identified a previously known number, conducted some additional research that the field office likely had already done, and disseminated the information back to the field as new reporting. Because the analysts could not fully explain the source of the intelligence, the agent did not realize the [redacted] reporting in fact reflected a new foreign connection to the telephone number. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

Another frustration voiced by agents to the [redacted] analysts was that leads disseminated under the project that were designated "Action leads" frequently did not yield significant investigative results, such as identifying new persons of interest or contributing to an active investigation. [redacted] b1, b3, b7E

[76] For example, circular reporting might have occurred when the FBI passed a Stellar Wind-derived telephone number or e-mail address to another agency within the U.S. Intelligence Community, that agency in turn requested the NSA to analyze the information, and the NSA subsequently disseminated the results back to the FBI in a Stellar Wind report. ~~(TS//STLW//SI//OC/NF)~~

[redacted]

~~(TS//STLW//SI//OC/NF)~~

The NSA responded to this frustration by implementing the [redacted] rankings described earlier to provide the agents some guidance on prioritizing the tippers. In addition, the FBI analysts told us that they became more adept at telephone analysis and "got better at their game" by eliminating low value tippers [redacted] from being disseminated to field offices. According to FBI documents, the FBI also sought additional information from the NSA about tippers ranked [redacted] before the FBI disseminated these tippers to the field for investigation. ~~(TS//STLW//SI//OC/NF)~~

3. FBI's Efforts to Track Stellar Wind Tippers and Update Executive Management on Status of [redacted] Leads ~~(S//NF)~~

b1, b3, b7E

Typically, FBI ECs originate from a specific investigative or administrative case file number. A file number is also required for an EC to be loaded into the FBI's Automated Case Management System and to enable the sending office to assign a lead to the receiving office. However, FBI Headquarters did not initially open an investigative file for the [redacted] ECs that disseminated Stellar Wind tippers to field offices. One of the original analysts assigned to the project told the OIG that he was familiar with a telephone analysis project in the FBI's drug program and that as a result he decided to issue the first Stellar Wind-related EC from that drug investigative file. This confused some field offices receiving the earliest ECs because counterterrorism leads were being disseminated under a drug investigation file number. ~~(TS//STLW//SI//OC/NF)~~

b1, b3, b7E

In mid-October 2001, the FBI created a subfile under the FBI's investigation of the September 11 terrorist attacks to disseminate Stellar Wind information. The FBI used this subfile, referred to as the [redacted] until September 2002, when a more formal program for disseminating Stellar Wind information, called [redacted] was created.[77] ~~(TS//STLW//SI//OC/NF)~~

b1, b3, b7E

The [redacted] analysts also told us that they created a database to attempt to track the status of leads disseminated to the field offices. The database identified each tipper by field office and the status of the lead that was assigned. One analyst stated that the response rate from

b1, b3, b7E

[77] We describe this more formal program in Chapter Six of this report. (U)

field offices was uneven during these early months, and their supervisors instructed the analysts at one point to contact the head of each field office to determine the status of the [redacted] leads for which each office was responsible. ~~(S//NF)~~ b1, b3, b7E

The [redacted] analysts used the database they created to produce status reports for senior FBI officials who were read into the Stellar Wind program. These reports provided statistics regarding the quantity and rankings of disseminated tippers, as well as brief synopses of the status of the [redacted] leads. The Stellar Wind program was viewed as an emergency response to the September 11 attacks and these status reports were intended to provide FBI executives information about how the program was contributing to the FBI's counterterrorism efforts. ~~(TS//SI//NF)~~ b1, b3, b7E

IV. Justice Department Office of Intelligence Policy and Review's (OIPR) and FISA Court's Early Role in Stellar Wind ~~(TS//STLW//SI//OC/NF)~~

When the President signed the first Authorization for the program on October 4, 2001, only two Department officials outside the FBI were read into the Stellar Wind program: Attorney General John Ashcroft, who certified the Authorization as to form and legality; and John Yoo, the Deputy Assistant Attorney General in the Office of Legal Counsel responsible for advising the Attorney General on the matter and for drafting the Department's first memorandum on the legality of the program.[78] The Department's Office of Intelligence Policy and Review (OIPR), despite its expertise in FISA matters, was not asked to consider how FISA might affect the program's legality or implementation, nor was OIPR asked to consider how the program might affect the Department's FISA operations. ~~(TS//SI//NF)~~

In this section, we provide an overview of OIPR, how James Baker, the head of OIPR, inadvertently came to learn about Stellar Wind soon after it was initiated, and the subsequent role that OIPR played in the program's operation. We also describe the circumstances surrounding the decision to have the FISA Court Presiding Judge and his successor read into the Stellar Wind program, and the Court's response to the program. ~~(TS//STLW//SI//OC/NF)~~

[78] Levin told us that he did not believe Yoo was read into Stellar Wind before the October 4, 2001, Presidential Authorization was signed, and we were not able to determine precisely when Yoo's read-in occurred. However, Yoo's November 2, 2001, memorandum analyzes the legality of the October 4, 2001, Authorization and the draft of the November 2, 2001, Authorization. Thus, it appears that Yoo was read into the program not later than November 2, 2001. ~~(TS//STLW//SI//OC/NF)~~

A. Overview of OIPR (U)

At the time of the implementation of the Stellar Wind program, OIPR was responsible for advising the Attorney General on matters relating to the national security activities of the United States.[79] Created shortly after enactment of the Foreign Intelligence Surveillance Act of 1978, OIPR reviewed executive orders, directives, and procedures relating to the intelligence community, and approved certain intelligence-gathering activities. OIPR also provided formal and informal legal advice to the Attorney General and U.S. intelligence agencies regarding questions of law and procedure relating to U.S. intelligence activities. In addition, OIPR advised the Attorney General and agencies such as the CIA, FBI, and Defense and State Departments concerning questions of law relating to U.S. national security activities and the legality of domestic and overseas intelligence operations. (U//~~FOUO~~)

OIPR also represented the United States before the FISA Court. OIPR was responsible for preparing and presenting applications to the FISA Court for orders authorizing electronic surveillance and physical searches by U.S. intelligence agencies for foreign intelligence purposes in investigations involving espionage and international terrorism. When evidence obtained under FISA was proposed to be used in criminal proceedings, OIPR sought the necessary authorization from the Attorney General, and in coordination with the Criminal Division and U.S. Attorney's Office prepared the motions and briefs required by the federal court whenever surveillance under FISA was challenged. (U)

The head of OIPR was referred to as the Counsel for Intelligence Policy and was supported by two Deputy Counsel and a staff of attorneys, paralegals, and administrative professionals. James Baker served as the Counsel for OIPR from May 2001 to January 2007.[80] (U)

B. OIPR Counsel Learns of Stellar Wind Program (U//~~FOUO~~)

Baker told us that while standing outside the Department one evening several weeks after the September 11 attacks, he was approached by an FBI colleague who said, "There is something spooky going on," that it appeared

---

[79] In September 2006, the Justice Department moved OIPR into the newly created National Security Division (NSD). In April 2008, NSD modified OIPR's structure and name. The new organization is called the Office of Intelligence and includes operations, oversight, and litigation sections. For purposes of this report we use the term OIPR to reflect the time period our review encompasses. (U)

[80] Baker served as Acting Counsel for OIPR from May 2001 to January 2002, and as Counsel from February 2002 until January 2007. Baker officially resigned from the Justice Department in October 2007. (U)

foreign-to-domestic collection was being conducted without a FISA order, and that some FBI personnel "were getting nervous." The FBI colleague asked Baker whether he knew anything about the activity, and Baker responded that he did not. ~~(TS//STLW//SI//OC/NF)~~

Baker said that while reviewing a FISA application several weeks after this conversation, a particular passage regarding international communications "leapt out at" him. According to Baker, the passage contained "strange, unattributed language" and information that was "not attributed in the usual way." Baker told the OIG that the information concerned connections between telephone numbers, but he could not recall if the information simply identified a link between individuals or also included the content of communications. ~~(TS//SI//NF)~~

Baker asked the OIPR attorney responsible for the application about the information in the passage, and the attorney responded that nobody at the FBI would disclose where the information had come from, only that it was part of a "special collection." Baker therefore contacted the FBI about the application. Unable to obtain any answers to his questions, Baker informed the FBI that he would not allow the application to be filed with the FISA Court. Baker said that, to the best of his recollection, he did not believe the application was filed with the Court. ~~(TS//SI//NF)~~

Soon thereafter, Baker spoke with Daniel Levin, who at that time was serving as both Counselor to the Attorney General and Chief of Staff to the FBI Director. Levin told Baker that approval from the White House was needed before he could tell Baker about the special collection. Levin told us that he successfully pressed the White House for Baker to be read into Stellar Wind. Baker stated that David Addington, counselor to Vice President Cheney, was the individual who approved his clearance into the program. ~~(TS//STLW//SI//OC/NF)~~

According to NSA records, Baker was read into Stellar Wind in January 2002.[81] He said his read in essentially consisted of Levin providing him a short briefing and a copy of Yoo's November 2, 2001, memorandum regarding the legality of the program. Baker told us that his initial reaction was that the program, and Yoo's memorandum, were flawed legally. Baker said he did not consider himself a constitutional law scholar, but was

---

[81] Baker told us that he initially was read into the program in December 2001 by Levin. Baker said he later received a more formal briefing on the program at the NSA, where he was allowed to read the Presidential Authorizations and discuss the program with NSA attorneys. This formal briefing appears to be the event that the NSA considers Baker's official read-in, which according to NSA records occurred on January 11, 2002. We used this date for purposes of calculating the number of Justice Department employees read into the program. (U//~~FOUO~~)

nevertheless surprised that while Stellar Wind was in his view "overriding a criminal statute" on the basis of the President's power as Commander in Chief, Yoo's memorandum did not even cite an important U.S. Supreme Court opinion on presidential authority during wartime, *Youngstown Sheet & Tube Co.* Baker said he believed that it is important to exercise some "humility" when dealing with national security matters because of the complexity and importance of the issues, and he therefore reserved final judgment on the memorandum until he researched the legal issues further. Yet, Baker said his initial opinion that the memorandum was flawed legally did not change over time. ~~(TS//STLW//SI//OC/NF)~~

We asked Baker whether at the time he thought the collection authorized under Stellar Wind could have been accomplished under FISA. Baker said that his thinking on this issue has evolved over time, but that he staunchly believed that "FISA works in wartime." He stated that although it is difficult to do, FISA can be made to work under the circumstances that existed following the September 11 attacks, but that it also was easy to "make FISA not work" under these circumstances.
~~(TS//STLW//SI//OC/NF)~~

Baker cited a lack of resources as the primary impediment to using the FISA process, rather than Stellar Wind, to collect foreign intelligence following the September 11 attacks. Baker said that he did not believe OIPR, as staffed in October 2001, had sufficient resources to process the volume of telephone numbers the NSA was tasking for content collection under Stellar Wind at that time. However, Baker explained that in his view FISA is "scalable" and that to some degree the statute's utility is limited by the resources allocated to OIPR.[82] ~~(TS//STLW//SI//OC/NF)~~

Baker also observed that to bring Stellar Wind's content and meta data collections fully under FISA authority would have required a different approach to the statute. Baker said that developing such an approach would have been possible only by convening a working group to examine constitutional and practical issues. Baker, one of only three people in the Justice Department read into Stellar Wind as of January 2002, said he did not have the ability or the authority to do this himself.[83] Baker stated that his belief in this approach was informed by his own experience with and participation in a small, informal group composed of U.S. Intelligence Community officials that had worked periodically since shortly before the

---

[82] Baker also observed that OIPR could have been staffed with detailees from the Department of Defense and other components within the Justice Department. (U)

[83] Baker also said that he did not have the legal resources within OIPR to "challenge" Yoo's November 2, 2001, legal analysis of the Stellar Wind program, although he believed it was flawed. ~~(TS//STLW//SI//OC/NF)~~

September 11 terrorist attacks to develop solutions to various foreign intelligence collection issues.[84] ~~(TS//STLW//SI//OC/NF)~~

C. FISA Court is Informed of Stellar Wind ~~(TS//SI//NF)~~

Baker told the OIG that sometime in the December 2001 to January 2002 time period he concluded, based on his awareness that information derived from Stellar Wind had been used to support at least one request for a FISA application, that the FISA Court also needed to be made aware of the Stellar Wind program. Baker said that the Department's counterterrorism efforts rely on good relations with the FISA Court and that candor and transparency are critical components of that relationship. According to Baker, OIPR had a policy of full disclosure with the Court that he said served the Department well when problematic issues arose. Baker also attributed the Department's record of success with FISA applications and the improved coordination between intelligence agents and prosecutors to the strong relationship that the Department had built with the Court. Baker believed it would be detrimental to this relationship if the Court learned later that information from Stellar Wind was included in FISA applications without notice to the Court. ~~(TS//STLW//SI//OC/NF)~~

Baker said he raised the issue of the FISA Court not being informed about Stellar Wind with Levin, who first responded by suggesting that the Attorney General order Baker not to disclose the program to the Court while the issue was being considered. Baker initially agreed to this approach and drafted a memorandum from Ashcroft to Baker to this effect. He said that Levin edited the document and presented it to Ashcroft, who signed it. The memorandum, dated January 17, 2002, stated that Ashcroft understood FISA Court applications would include information obtained or derived from Stellar Wind, and that these applications would seek authorizations to conduct surveillance of targets already subject to surveillance under Stellar Wind. Ashcroft's memorandum also stated that he was considering Baker's recommendation that the Department brief the FISA Court on the program. The memorandum stated further:

> In the interim, I am directing you to file applications with the Foreign Intelligence Surveillance Court without informing the court of the existence of the Stellar Wind program or any aspect thereof. I am also directing you not to brief any other

---

[84] This type of collaborative effort ultimately developed the legal theories used to transition Stellar Wind's collection activities to FISA authority. However, as we discuss in Chapter Five, while the transition was successful with respect to bulk meta data collection, the legal theory to transition Stellar Wind's content collection, while initially approved by one FISA Court judge, subsequently was rejected by a second judge. ~~(TS//STLW//SI//OC/NF)~~

individuals in the Department of Justice, including the FBI, regarding Stellar Wind without my prior authorization. ~~(TS//STLW//SI//OC/NF)~~

Levin told us that he, as well as Ashcroft, soon came to agree with Baker that the FISA Court should be made aware of the program. Levin said he told Ashcroft during this time that Baker had done a "remarkable job" building a relationship with the FISA Court that greatly benefited the Department's counterintelligence and counterterrorism efforts. Levin said he advised Ashcroft, "We should do what Baker thinks is right." According to Levin, Ashcroft agreed. ~~(TS//STLW//SI//OC/NF)~~

Levin said that he informed Gonzales and Addington at some point of Baker's position that the FISA Court should be made aware of Stellar Wind, but said they initially rejected the idea of reading any judges into the program. Levin stated that he continued to press the issue without success. ~~(TS//STLW//SI//OC/NF)~~

However, the issue came to a head on a weekend in January 2002 when Baker reviewed a second FISA application that contained the "strange, unattributed language" Baker understood to indicate that the information referenced was obtained from the Stellar Wind program. This second FISA application sought emergency approval from the FISA Court to conduct electronic surveillance of [redacted] Because this would be the first application seeking FISA authority to monitor this particular subject's telephone communications, Baker recognized that the NSA had already engaged in some level of electronic surveillance in the United States of a domestic telephone number without a FISA order. ~~(TS//STLW//SI//OC/NF)~~

Although Baker viewed the memorandum from Ashcroft directing him not to inform the FISA Court about Stellar Wind as "cover" for him not to inform the FISA Court about Stellar Wind, he remained uncomfortable about filing an application that contained Stellar Wind information without informing the FISA Court. Baker therefore approached the Chief of the Justice Department's Professional Responsibility Advisory Office (PRAO) to discuss his ethical responsibilities to the FISA Court under circumstances where a FISA application contains certain information that is material to the Court's decision, but Baker was not authorized to disclose the source of the

information.[85] Baker stated that the PRAO Chief told him that he had an affirmative duty of candor to the Court, and that this duty of candor was heightened due to the *ex parte* nature of the FISA proceedings.[86] Baker concurred with this guidance, which Baker felt also was compelled by his position as a federal officer and officer of the Court. Baker said he therefore concluded, and informed Levin, that he would not sign the pending application or present to it to the FISA Court, nor would he allow any OIPR attorney do so. According to Baker, Levin spoke to David Addington about the situation, but Addington nevertheless declared that the Court would not be read into the program. ~~(TS//STLW//SI//OC/NF)~~

According to Baker, the White House, the Attorney General, and Levin then decided that Levin, rather than Baker, would sign the FISA application and present it to Judge Claude M. Hilton, the FISA Court judge responsible for hearing FISA matters that weekend.[87] Baker told us that he notified Judge Hilton in advance that the application was being handled in this manner. Levin said he brought the application to Judge Hilton's residence and explained that he, instead of the OIPR Counsel, was presenting the case because it involved a "special classified program." Levin told us that Judge Hilton approved the application without asking any questions. According to Levin, when he later told Addington how the matter was resolved, and that he agreed with Baker's position that the Court should be briefed into the program, Addington responded that Baker should be fired for insubordination for not signing the application. ~~(TS//STLW//SI//OC/NF)~~

According to Baker, a consensus formed after this episode among the Attorney General, the FBI, and the White House that future FISA matters could not be handled in the same fashion, particularly in view of the anticipated increase in FISA applications resulting from the intelligence collected and disseminated under Stellar Wind.[88] Baker said that the

---

[85] The Professional Responsibility Advisory Office provides advice to Department attorneys with respect to professional responsibility issues. (U)

[86] Baker cited Rule 3.3 of the American Bar Association's Model Rules of Professional Conduct as the specific rule implicated by the situation. That rule provides, in relevant part, that "in an ex parte proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer which will enable the tribunal to make an informed decision, whether or not the facts are adverse." Baker stated that he also consulted with two officials from the Office of the Deputy Attorney General on the matter and that they provided the same advice as PRAO. (U)

[87] Director Mueller and Attorney General Ashcroft already had signed the application. (U)

[88] We asked Baker whether he thought the FBI's restrictions on the use of Stellar Wind-derived leads disseminated to field offices, as described above, were sufficient to guard against including Stellar Wind information in FISA applications. Baker stated that his experience with FBI record-keeping practices did not give him a high degree of

(Cont'd.)

decision was therefore made to brief the FISA Court's Presiding Judge, Royce Lamberth.[89] ~~(TS//STLW//SI//OC/NF)~~

Judge Lamberth was read into Stellar Wind on January 31, 2002. The briefing was conducted in the Attorney General's office at the Department, and was attended by Ashcroft, Hayden, Mueller, Levin, Yoo, and Baker. According to a memorandum of talking points prepared for the briefing, Ashcroft provided Judge Lamberth a brief summary of the program's creation, explaining that the President had authorized a sensitive collection technique in response to the September 11 attacks in order to obtain foreign intelligence information necessary to protect the United States from future attacks and acts of international terrorism. Ashcroft said the NSA, at the instruction of the Secretary of Defense, implemented the collection, which was code named Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

According to the talking points, Ashcroft also discussed the factors the President considered in determining that an "extraordinary emergency exists" to support electronic surveillance without a warrant. The factors cited to Judge Lamberth paralleled those contained in the Presidential Authorizations, including "the magnitude and probability of death from terrorist attacks, the need to detect and prevent such attacks with secrecy, the possible intrusion into the privacy of American citizens, the absence of a more narrowly-tailored means to obtain the information, and the reasonableness of such intrusion in light of the magnitude of the potential threat of such terrorist acts and the probability of their occurrence." ~~(TS//STLW//SI//OC/NF)~~

According to the talking points, Ashcroft stated that he determined, based upon the advice of the Office of Legal Counsel, that the President's actions were lawful under the Constitution. Levin told us that Ashcroft emphasized to Judge Lamberth that the FISA Court was not being asked to approve the program. ~~(TS//STLW//SI//OC/NF)~~

Following Ashcroft's summary, the briefing continued in three parts. First, Hayden described how the program worked operationally. Second, Yoo discussed legal aspects of the program. Third, Baker discussed a

---

confidence that such separation could be consistently maintained. In addition, Baker believed that the nature of FBI international terrorism investigations would make it difficult to track Stellar Wind-derived information. According the FBI OGC, Baker did not share with the FBI his concerns about whether its record-keeping practices would keep Stellar Wind information from being used in FISA applications. ~~(TS//STLW//SI//OC/NF)~~

[89] The Presiding Judge for the FISA Court is appointed to a 7-year term by the Chief Justice of the Supreme Court of the United States. Judge Lamberth was appointed as Presiding Judge in 1995. (U)

proposal for handling FISA applications that contained program-derived information. ~~(TS//STLW//SI//OC/NF)~~

Levin told us that when the briefing concluded, Lamberth acknowledged he was not being asked to approve the program and expressed his appreciation for being read in. According to Baker, Lamberth also remarked, "Well, it all depends on whether you can get five votes on the Supreme Court, but I'm comfortable with it." For the next 4 months, until the end of his term in May 2002, Judge Lamberth was the only FISA Court judge read into Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

D. OIPR Implements "Scrubbing" Procedures for Stellar Wind Information in International Terrorism FISA Applications ~~(TS//STLW//SI//OC/NF)~~

Following Judge Lamberth's read-in to the Stellar Wind program, Baker implemented procedures in OIPR to address two scenarios in which Stellar Wind could affect international terrorism FISA applications.[90] First, information obtained or derived from Stellar Wind might be included in a FISA application to establish probable cause that the target of the application is a foreign power or an agent of a foreign power and that the target is using or is about to use a particular "facility" (a term used in FISA generally to refer to a specific telephone number or e-mail address) at which the electronic surveillance is directed. Second, a FISA application might target facilities that were also targeted by Stellar Wind, a situation referred to as "dual coverage" because the targeted communications were collected under two separate authorities. Baker's procedures, referred to as "scrubbing" procedures, applied to initial FISA applications as well as to renewal applications seeking to continue existing coverage of targets (electronic surveillance under FISA generally is authorized for 90-day periods). ~~(TS//STLW//SI//OC/NF)~~

Judge Lamberth required that all applications that contained NSA information derived from Stellar Wind or that would produce dual coverage of a facility be filed with him only. Baker told the OIG that the scrubbing process was his idea, with Judge Lamberth's full concurrence, and that it had as its core principle OIPR's obligation to inform the Court of all material facts contained in a FISA application. According to Baker, the scrubbing

---

[90] The procedures implemented by Baker only applied to international terrorism FISA applications, not to counterintelligence FISA applications. As Baker later explained in a letter to Judge Lamberth's successor as FISA Presiding Judge, this limitation was based on the understanding that the Stellar Wind program targeted only certain international terrorist communications "and there is no reason to believe that the fruits of Stellar Wind collection would appear in a counterintelligence FISA application." ~~(TS//STLW//SI//OC/NF)~~

procedures were a means of implementing his ethical duty of candor to the Court without disclosing the existence of the Stellar Wind program to uncleared attorneys and judges. Baker also said that Judge Lamberth wanted to be informed of applications that contained Stellar Wind information and of dual coverage situations, and that Judge Lamberth believed that the procedures devised by Baker were an appropriate and acceptable means of accomplishing this. According to Baker, the scrubbing process made him and Judge Lamberth "comfortable the Court was being told what it needed to be told."[91] ~~(TS//STLW//SI//OC/NF)~~

We describe below the initial two scrubbing procedures implemented by Baker as well as the difficulties they created for the FISA application process. ~~(TS//STLW//SI//OC/NF)~~

1. Initial Scrubbing Procedures ~~(TS//SI//NF)~~

Each international terrorism FISA application was "scrubbed" for Stellar Wind information and dual coverage before it was filed. However, Baker, as the only person in OIPR read into Stellar Wind, was unable to explain to his staff why the scrubbing was being conducted. With the NSA's cooperation, Baker initially scrubbed the applications without any assistance from OIPR staff. Baker said the time and effort he expended on this practice was not sustainable, and within weeks of beginning the scrubbing procedures Baker enlisted the assistance of OIPR's Acting Deputy Counsel for Intelligence Operations, Peggy Skelly-Nolen. Skelly-Nolen stated to the OIG that Baker told her at that time that he "needed to tell me something that he couldn't tell me," but was able to convey that he needed her and the office's assistance to process international terrorism FISA applications because the supporting declarations contained information that required special handling. ~~(TS//STLW//SI//OC/NF)~~

The scrubbing process, or "the program check" as it came to be known within OIPR, had two purposes. The first purpose was to identify draft applications that contained Stellar Wind-derived information in support of probable cause to believe that the target of the application was a foreign power or an agent of a foreign power and was using or was about to use a particular facility. The second purpose was to identify applications that targeted facilities that were already actively targeted under the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

---

[91] The FBI OGC told us that Baker never disclosed to it that the FISA Court was concerned about risks presented by the inclusion of Stellar Wind information in FISA applications, nor did Baker inform the FBI that OIPR implemented procedures to address these concerns. ~~(TS//STLW//SI//OC/NF)~~

To accomplish the first purpose, OIPR attorneys were required to identify any information in applications attributed to the NSA, even if there was no suggestion the information was derived from a special program. The OIPR attorneys provided by e-mail the relevant excerpts from the applications to a designated OIPR legal assistant, who in turn compiled the information and transmitted it to the NSA by secure e-mail or facsimile. Upon receipt, the NSA conducted a check of the identified information against the Stellar Wind reports database, among others, to determine whether the information was derived or obtained from the program (as distinguished from being obtained by some other NSA signals collection activity). The NSA provided OIPR the results of its search by return e-mail or facsimile, writing next to each excerpt either "yes" or "no" to indicate whether the information was Stellar Wind-derived. Judge Lamberth did not require that Stellar Wind-derived information be removed from FISA applications, only that any such applications be filed with him exclusively and the Stellar Wind information identified to him orally.[92]
~~(TS//STLW//SI//OC/NF)~~

The second purpose of the scrub – to identify dual collection applications – followed similar steps. On approximately a weekly basis, an OIPR legal assistant requested that OIPR attorneys transmit to him all facilities targeted for electronic surveillance in applications scheduled to be filed with the FISA Court that week. The legal assistant created a single list of all targeted telephone numbers and e-mail accounts and e-mailed or faxed the information to the NSA. The NSA in turn checked the Stellar Wind database to determine whether any of the listed facilities were tasked for content collection under the program. The NSA provided OIPR the results of this check by return e-mail or facsimile, writing next to each facility either "yes" or "no" to indicate whether the facility was tasked under Stellar Wind.
~~(TS//STLW//SI//OC/NF)~~

Baker proposed to Judge Lamberth that OIPR notify him of dual coverage cases by including in the applications a [redacted]

[redacted]

[92] Baker said that only [redacted] international terrorism FISA applications presented to Judge Lamberth included Stellar Wind information to support the application.
~~(TS//STLW//SI//OC/NF)~~

[redacted]

(Cont'd.)

[redacted] Baker proposed to include this descriptive phrase in applications that, if approved, would result in dual coverage. ~~(TS//STLW//SI//OC/NF)~~

Beginning in early 2002, any FISA applications that included the descriptive phrase [redacted] were to be presented to Judge Lamberth, [redacted] also would inform Judge Lamberth directly that it was a "Lamberth only" case to indicate it was connected to Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

2. Complications with Scrubbing Procedures ~~(TS//SI//NF)~~

Skelly-Nolen told us that no one in OIPR, including her at that time, was aware that the checks Baker was requiring the office to make concerned a specific compartmented program. However, the scrubbing procedures generated questions from OIPR attorneys and FBI agents, particularly when Skelly-Nolen instructed an OIPR attorney to add to an application the descriptive phrase [redacted] Skelly-Nolen told us that she was not able to provide a satisfactory response to the questions because she did not have the answers. ~~(TS//SI//NF)~~

Skelly-Nolen also stated that it was stressful to comply with the procedures, due in large part to the fact that the attorneys and agents responsible for the contents of the international terrorism applications were asked to follow certain procedures for filings but were not being provided an explanation for these measures. She said this stress was compounded by the concurrent anthrax scare and the prevailing belief that there would be another terrorist attack. Skelly-Nolen stated that OIPR staff was acting based on Baker's representations alone, and while Baker sought to assuage any concerns the OIPR attorneys had over these new procedures by

[redacted]

explaining to the office that he had spoken to the Attorney General and the FISA Court on the issue, some OIPR attorneys simply were not comfortable under these circumstances and Skelly-Nolen had to reassign the international terrorism cases these attorneys were handling. Baker stated that he regularly told attorneys that they did not have to sign applications that they were not comfortable with. ~~(TS//SI//NF)~~

The process for filing international terrorism FISA applications was further complicated by the fact that of the two Justice Department officials authorized to approve such applications – the Attorney General and the Deputy Attorney General – only Attorney General Ashcroft was read into Stellar Wind.[94] As mentioned previously, Larry Thompson, who served as Deputy Attorney General from May 2001 to August 2003, was never read into the Stellar Wind program. Alberto Gonzales, who served as White House Counsel from January 2000 to February 2005, stated to the OIG that he recalled that Ashcroft wanted Thompson, as well as Ashcroft's Chief of Staff, read into Stellar Wind, but that neither official ever was. Gonzales said Ashcroft complained that it was "inconvenient" not having these two officials read into the program.[95] ~~(TS//STLW//SI//OC/NF)~~

The situation with Thompson caused Associate Deputy Attorney General David Kris, who oversaw national security matters in the Office of the Deputy Attorney General during Thompson's tenure, to draft a memorandum on January 11, 2002, advising Baker that he should not send Kris any FISA applications that included information obtained or derived from the Stellar Wind program, and that Kris intended to advise Thompson not to review or approve any such applications.[96] The memorandum stated that Kris was aware of the existence of a "highly classified information-collection program that has the unclassified code name 'Stellar Wind'," but that he was "wholly unaware of the nature and scope of the

---

[94] Each FISA application must be approved by the Attorney General, defined under § 1801(g) to include the Deputy Attorney General or Acting Attorney General, based on the Attorney General's finding that the application "satisfies the criteria and requirements of such application as set forth in [subchapter I concerning electronic surveillance]." 50 U.S.C. § 1804(a). (U)

[95] As noted above, Gonzales also told the OIG that he never got the sense from Ashcroft that the situation affected the quality of the legal advice the Department provided to the White House. However, as described in Chapter Four, others had a decidedly different impression of Ashcroft's opinion of the legal advice he received on Stellar Wind during this period. We were unable to interview Ashcroft about this issue. ~~(TS//SI//NF)~~

[96] Baker told the OIG that he had informed Kris about the existence of a classified program that he could not discuss further, and that it impacted FISA applications. Baker said he and Kris agreed that, under the circumstances, it was not appropriate for Thompson to sign applications if he was not fully informed about all of the material facts related to them. ~~(TS//SI//NF)~~

program." Kris also stated in the memorandum that his request for a briefing on the program had been denied and that he was aware Deputy Attorney General Thompson also had not been briefed on the program.[97] ~~(TS//STLW//SI//OC/NF)~~

E. Judge Kollar-Kotelly Succeeds Judge Lamberth as FISA Court Presiding Judge (U)

Judge Lamberth's 7-year term on the FISA Court ended in May 2002. On May 19, 2002, Judge Colleen Kollar-Kotelly was appointed to the Court to replace Lamberth as the Presiding Judge. In connection with this appointment, Judge Kollar-Kotelly was read into the Stellar Wind program and provided an opportunity to examine the Department's analysis of the program's legality. Judge Kollar-Kotelly also spoke with Baker on numerous occasions about the scrubbing procedures he implemented to account for Stellar Wind information in international terrorism FISA applications and to identify applications that would result in dual coverage. ~~(TS//STLW//SI//OC/NF)~~

1. Judge Kollar-Kotelly Modifies OIPR Scrubbing Procedures ~~(TS//SI//NF)~~

Judge Kollar-Kotelly received her first briefing on the Stellar Wind program in the Attorney General's office on May 17, 2002, 2 days prior to being formally appointed Presiding Judge for the FISA Court. Baker, who attended the briefing, told us that the presentation was similar to the briefing initially provided to Judge Lamberth. Judge Kollar-Kotelly had several questions concerning the scope of the President's authority to conduct warrantless surveillance, and the Department responded that same day with a letter signed by OLC Deputy Assistant Attorney General Yoo that outlined the legal basis for the activity. The letter essentially replicated Yoo's November 2, 2001, memorandum regarding the legality of Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

According to Baker, Judge Kollar-Kotelly met at the White House with Addington, Gonzales, and Yoo to read Yoo's letter, but she was not permitted to retain a copy or take any notes. Judge Kollar-Kotelly later wrote in a letter to Baker that Yoo's letter "set out a broad overview of the legal authority for conducting [Stellar Wind], but did not analyze the specifics of the [Stellar Wind] program." ~~(TS//SI//NF)~~

[97] [redacted]
~~(TS//SI//NF)~~

Judge Kollar-Kotelly also requested an opportunity to review the Presidential Authorization initiating Stellar Wind. On August 12, 2002, she reviewed the October 4, 2001, Authorization. ~~(TS//SI//NF)~~

Baker said that he met with Judge Kollar-Kotelly on several occasions after her initial Stellar Wind briefing to discuss how OIPR had been handling Stellar Wind's impact on FISA applications. Baker described for her the existing procedures to account for NSA information contained in FISA applications derived from Stellar Wind, and to identify applications that, if approved, would produce dual coverage of a facility. ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly also was interested in identifying whether a facility targeted in a FISA application had been tipped to the FBI as Stellar-Wind derived information. Baker told the OIG that at this time he did not believe the FBI and NSA had the ability to track Stellar Wind tips on a timely basis. Baker said he mistakenly believed that as tips passed from the NSA to FBI Headquarters, and from there to FBI field offices for investigation, it would be exceedingly difficult to trace the specific source of the information in a sufficiently timely manner for inclusion in a FISA application. Baker provided his understanding to Judge Kollar-Kotelly, likening the Stellar Wind information in tips to the FBI as "salt in soup" that is impossible to extract once added. Based on Baker's representations, Judge Kollar-Kotelly did not require the Department to identify whether a facility targeted in a FISA application was ever provided to the FBI under Stellar Wind.[98] ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly decided that the scrubbing procedures implemented under Judge Lamberth should continue, but she directed OIPR to discontinue including in applications the descriptive phrase [redacted] as a means of notifying her that facilities targeted by the applications were also targeted under Stellar Wind. Baker said that while Judge Kollar-Kotelly understood that instances of dual coverage would occur, she did not want to appear to judicially sanction Stellar Wind coverage. Baker told us his impression was that Judge Kollar-Kotelly "did not want to rule on the legality of the program" by appearing to "authorize" the NSA's technique for collecting the same information the government was seeking to collect under FISA.[99]

---

[98] Baker eventually learned that the FBI and the NSA in fact did have some ability to track Stellar Wind information. As discussed in Chapter Six, in March 2004 Judge Kollar-Kotelly added to the scrubbing process a check performed by the FBI to determine whether any telephone numbers or e-mail addresses contained in a FISA application had ever been provided to the FBI in a Stellar Wind report. ~~(TS//STLW//SI//OC/NF)~~

[99] Judge Kollar-Kotelly later wrote about the dual coverage issue, in a January 12, 2005, letter to Baker that discussed the "Stellar Wind Program and Practice Before the (Cont'd.)

Baker said he believes Judge Kollar-Kotelly was trying to protect the FISA Court and did not want the legality of the Court's orders called into question. ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly also directed OIPR to excise from FISA applications any information obtained or derived from Stellar Wind. Baker told Judge Kollar-Kotelly that OIPR could implement this requirement using the scrubbing procedures already in place, and that where the FBI included NSA information in an application determined to be Stellar Wind-derived, OIPR would excise it. ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly also instructed Baker to alert her of any instances where an application's basis for the requisite probable cause showing under FISA was weakened by excising the Stellar Wind information. In such cases, Judge Kollar-Kotelly would then decide whether to approve the application with the knowledge that additional relevant information had been excised. ~~(TS//STLW//SI//OC/NF)~~

Even though Judge Kollar-Kotelly's scrubbing process was intended to eliminate all Stellar Wind information from international terrorism FISA applications, she still required that scrubbed applications be filed with her only. In time, Judge Kollar-Kotelly relaxed this requirement and permitted other judges on the Court to handle these applications, although only after first being filed with her.[100] ~~(TS//STLW//SI//OC/NF)~~

2. OIPR implements Judge Kollar-Kotelly's Scrubbing Procedure ~~(TS//SI//NF)~~

According to Baker and Skelly-Nolen, the mechanics within OIPR for determining whether an application contained Stellar Wind information or targeted a facility also targeted under Stellar Wind remained essentially unchanged after the transition from Judge Lamberth to Judge Kollar-Kotelly. However, the scrubbing process became more complex. For

---

FISC." The letter memorialized the information Judge Kollar-Kotelly received from the government about the program and how she requested the government to proceed in preparing and presenting applications. On the subject of dual coverage, Judge Kollar-Kotelly wrote, "Without opining on [Stellar Wind]-related legal issues, I have sought to protect the proper functioning of the FISA process, under which separate court authorities are granted to conduct foreign intelligence collection against a set of targets that overlaps the set of [Stellar Wind] targets." We discuss this letter in Chapter Four of this report. ~~(TS//STLW//SI//OC/NF)~~

[100] [redacted]

example, because only the Attorney General could sign the applications and Judge Kollar-Kotelly required that only she receive the applications (even after being scrubbed), Skelly-Nolen had to regularly visit the Attorney General's and Presiding Judge's residences with stacks of what Skelly-Nolen came to refer to as "AG-KK only" FISA applications. ~~(TS//STLW//SI//OC/NF)~~

The situation was further complicated when Ashcroft was on overseas travel and his signature was needed for a scrubbed application ready to be filed. When this occurred, the classification of the application's signature page was "downgraded" and then sent to Ashcroft by secure fax. The actual application was not faxed; instead, Skelly-Nolen typically included a statement from her or Baker with the signature page indicating that the application was proper and complied with the requirements of the FISA statute. Skelly-Nolen observed that in these cases Ashcroft essentially relied on her and Baker's assessments of the applications – even though Skelly-Nolen was not read into Stellar Wind at this time. Scrubbed applications were handled similarly when Ashcroft was traveling domestically, although in those instances the applications could be provided along with the signature page if requested.[101] ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly also required that hearings for the "AG-KK only" FISA applications and renewals be scheduled for late in the day or on the weekend, either in her courtroom chambers at the District Court for the District of Columbia or at her residence. According to Skelly-Nolen, Judge Kollar-Kotelly insisted on this practice so that the "AG-KK only" docket did not interfere with her regular court docket. From Skelly-Nolen's perspective, this practice proved to be an "enormous burden," particularly in cases involving applications to continue FISA coverage on targets of emergency authorizations.[102] Skelly-Nolen explained that these authorizations were, for "no good operations reason" that she was aware of, routinely approved by the Attorney General on Fridays, meaning that a FISA application had to be filed with the Court within 72 hours – by Monday – to continue the emergency surveillance coverage. However, because Judge Kollar-Kotelly had a regular court docket on Mondays, she required that any scrubbed FISA application seeking authority to continue surveillance initiated under

---

[101] Baker and Skelly-Nolen told the OIG that in their experience it was not unusual for an Attorney General or Deputy Attorney General to rely on OIPR's representations that the FISA applications presented for signature satisfied the statute's requirements, instead of reviewing the full contents of each application. (U//~~FOUO~~)

[102] As previously described, under FISA during this time period, when the Attorney General reasonably determines that an emergency situation exists prior to obtaining a FISA order, the Attorney General may approve the use of electronic surveillance for a period of up to 72 hours without an order. (U)

emergency authorization be scheduled with her for Sunday. Skelly-Nolen stated that these cases would be in addition to the renewal applications that also had to be heard on Sundays so the authority for the surveillance in those cases did not expire and the coverage lapse.
~~(TS//STLW//SI//OC/NF)~~

Baker identified another issue that stemmed from Judge Kollar-Kotelly's requirement that only she receive dual coverage applications. The problem arose when Judge Kollar-Kotelly was out of town and unavailable to hear a dual coverage application. Baker's solution was either to fly the application to the place Judge Kollar-Kotelly was located, or to contact the NSA and request that it "de-task" the facilities that the FISA application was targeting. In this way, the application could be presented to an alternative FISA Court judge because it no longer targeted facilities that were also targeted under Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

For example, Baker described a situation where the FBI was urgently interested in a particular individual whose telephone was currently tasked by the NSA under Stellar Wind. In this case, Baker instructed the NSA to de-task the telephone number so the FBI's FISA application could be presented to a judge other than Judge Kollar-Kotelly. To prevent any gap in coverage between the time the NSA detasked the telephone number and the Court approved the FBI's application, surveillance was initiated under FISA's emergency authorization provision and then presented to a FISA Court judge within the requisite 72 hours. According to Baker, proceeding in this fashion "made everyone comfortable," including the NSA. Baker told us that this situation occurred a couple of times each year.
~~(TS//STLW//SI//OC/NF)~~

According to Baker and Skelly-Nolen, these examples illustrate how having only the Attorney General and a single judge on the FISA Court read into Stellar Wind complicated the FISA process. Baker said that "fairly early on" after being read into the program, Judge Kollar-Kotelly made several requests for other FISA Court judges to be read into the program. Baker told the OIG that these requests were generally made through him, orally and in writing, but was aware that on at least one occasion Judge Kollar-Kotelly made the request directly to Attorney General Ashcroft. Baker said that sometime prior to March 2004 he personally advised Ashcroft of Judge Kollar-Kotelly's concerns, and that Ashcroft responded with words to the effect that the White House would not allow more judges to be read into Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

In a January 12, 2005, letter to Baker, Judge Kollar-Kotelly summarized the situation, stating, "I have repeatedly asked that the other members of the FISC be given access to the same information that I have received regarding the [Stellar Wind] program. To date, the executive

branch has declined to do so, citing a need to maintain the strictest secrecy regarding [Stellar Wind]." ~~(TS//STLW//SI//OC/NF)~~

As a consequence of only Judge Kollar-Kotelly being read into Stellar Wind and her insistence that she alone handle applications scrubbed of Stellar Wind information or that involved tasking telephone numbers or e-mail addresses already tasked under Stellar Wind (dual coverage), by November 2004 she was handling approximately [redacted] percent of all FISA applications. Judge Kollar-Kotelly also tended to hear successive applications regarding the same targeted facilities. She discontinued this practice in November 2004 and permitted other judges to hear scrubbed applications. Judge Kollar-Kotelly later wrote that her decision was "based on the operational systems" OIPR had in place to scrub applications and that she assured her colleagues "that they could properly decide [the cases] based on the information in each application, without the additional information on which I have been briefed, but which, to date, the other judges have not received." ~~(TS//STLW//SI//OC/NF)~~

V. FBI Initiates Measures to Improve the Management of Stellar Wind Information ~~(S//NF)~~

Following the terrorist attacks of September 11, the FBI had reallocated personnel and resources to counterterrorism operations, and established the Telephone Analysis Unit (TAU) to exploit telephone communications data. We described above how a small team of agents and analysts from this unit was reassigned to the [redacted] which was responsible for handling the Stellar Wind reports provided by the NSA. ~~(S//NF)~~ b1, b3, b7E

In approximately May 2002, the TAU was renamed the Communications Analysis Unit (CAU) and became one of the units within the newly created Communications Exploitation Section (CXS). According to the first Acting CAU Unit Chief, the FBI's vision for the unit was that it would support FBI international terrorism investigations by [redacted] The Stellar Wind program was one source for obtaining this [redacted] ~~(S//NF)~~

In this section, we describe changes the FBI implemented in late 2002 and early 2003 to manage the intelligence it received under Stellar Wind. These changes included attempts to improve coordination with the NSA, implement a more formal program to receive intelligence from the NSA and disseminate it to FBI field offices, educate the FBI field offices about the value of the intelligence and FBI Headquarters' expectations concerning its use, and assign a small team of FBI personnel to work full-time at the NSA on Stellar Wind. ~~(S//NF)~~

A. CAU Acting Unit Chief Evaluates FBI Response to Stellar Wind ~~(S//NF)~~

When the first CAU Unit Chief arrived at FBI Headquarters in September 2002, CXS was newly established and most of the Section's 15-20 staff was there on temporary duty assignments. The CAU was staffed similarly at this time, but also contained some professional support employees from other divisions at FBI Headquarters. ~~(S//NF)~~

The CAU Unit Chief said that the CAU's mission was to support FBI international terrorism investigations – al Qaeda investigations in particular – by analyzing telephone calling activity and e-mail communications. He explained that prior to September 11, 2001, the FBI analyzed telephone numbers received by field offices or other sources by querying the numbers against the FBI's [redacted] database, the FBI's central repository for telephone subscriber data. However, he said the FBI's database at that time was relatively small and had limited analytical capability. In the wake of the September 11 attacks, the FBI gained access to additional tools and began to utilize more sophisticated analytical techniques. Stellar Wind was one of those new tools. b1, b3, b7E
~~(TS//STLW//SI//OC/NF)~~

The CAU Unit Chief said that after he was read into Stellar Wind in late September 2002, it was clear to him based on conversations with the CXS Acting Section Chief that the FBI wanted to increase its participation in the Stellar Wind program. As a counterterrorism agent in the FBI's Chicago field office, the Unit Chief had some exposure to Stellar Wind in the form of [redacted] leads. He told us that he had recalled thinking the leads were "stupid" and "not sensible." He also said that he had been critical of the leads because they did not provide any context to the information, such as how it was obtained. He stated that the leads did not adequately explain the [redacted] rankings associated with the telephone numbers, and the leads were not sufficiently specific as to what action the field office was expected to take. In his view, the intelligence disseminated by the [redacted] ECs was not "actionable." The Unit Chief told us that he could not figure out why FBI Headquarters was "pushing this stuff out" after September 11, and that other agents in the field shared his views.[103] b1, b3, b7E
~~(TS//STLW//SI//OC/NF)~~

[103] As previously described, former NSA Director Hayden told us that immediately following the September 11 terrorist attacks the NSA modified the agency's collection [redacted] and that this resulted in a flood of telephone numbers to the FBI. Thus, it is possible that (Cont'd.)

After becoming the acting Unit Chief for the CAU and reviewing how the FBI was handling the Stellar Wind information, he learned that there was no unit that oversaw the [redacted] and no guidance for how the NSA information should be processed by FBI analysts. He also said that the process in place – essentially re-typing into ECs the tearline information contained in Stellar Wind reports – merely "regurgitated" information that, by itself, was not actionable. He was not critical of the FBI analysts responsible for drafting the ECs, who simply performed this task as directed. Rather, he believed the process suffered from a lack of leadership. He described the FBI's involvement in Stellar Wind up to this point as "happenstance" and said the FBI did not have "a real good handle on it." He said that the deficiencies he identified were attributable in part to the significant resource challenges the FBI encountered after September 11, but he nevertheless considered the FBI's effort to respond to the Stellar Wind information as "half-baked." He said he therefore set about implementing changes within the CAU to better organize this effort, which he believed would improve the quality of the intelligence disseminated to FBI field offices. ~~(TS//STLW//SI//OC/NF)~~

b1, b3, b7E

B. FBI Increases Cooperation with NSA and Initiates [redacted] Project to Manage Stellar Wind Information ~~(TS//STLW//SI//OC/NF)~~

b1, b3, b7E

The CAU Unit Chief said that the first step he took to improve the FBI's involvement in Stellar Wind was to detail to the NSA one of CAU's temporary duty special agents. He instructed the agent to form a working group at the NSA to identify any problems and evaluate the quality of the information provided in the NSA's Stellar Wind reports, as well as the information that the FBI reported back to the NSA about tips.[104] The CAU Unit Chief said he took this step so that the NSA gained a "case agent's perspective" on the type of information useful to FBI field offices, and also to explain to the NSA that the information that could be disseminated about the tippers should include "context" and "clarity" sufficient to justify the FBI conducting an inquiry under the FBI's investigative guidelines.[105] He said he did not believe that the NSA's interest in obscuring the "sources and methods" associated with the information had to compromise the quality of the information provided to the FBI. He also said that the NSA needed to

---

FBI agents' early frustration with leads that provided telephone numbers was attributable in part to the leads generated under this NSA collection activity. ~~(TS//STLW//SI//OC/NF)~~

[104] The CAU Unit Chief recalled that the NSA had expressed frustration that the FBI never provided the NSA any responses to the tipped information. ~~(S//NF)~~

[105] FBI international terrorism investigations at this time were governed by the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations. (U)

understand how the FBI investigated intelligence that it received, and that FBI agents did not have to know the specific sources and methods used to acquire information in order to effectively investigate the information. ~~(S//NF)~~

The CAU Unit Chief said that this liaison effort occurred over a couple of weeks, with the temporary duty agent driving to the NSA daily. According to the Unit Chief, the agent explained to NSA personnel what the FBI was permitted to do with certain types of information and that the NSA would receive more feedback from the FBI if the quality of the disseminable information about the tippers improved. The Unit Chief told us that following this exchange the NSA improved the Stellar Wind reports by providing better information in both the compartmented and tearline portions of the reports. ~~(S//NF)~~

In addition, the CAU Unit Chief told us that he took steps to increase cooperation within the FBI between CAU, which was part of an analytical section that supported counterterrorism investigations, and FBI Headquarters' International Terrorism Operations Section, which was responsible for overseeing FBI counterterrorism investigations. The Unit Chief said that based on his experience in the field working counterterrorism cases, he believed it was important that the CAU analysts consult with agents in the operational section about leads the CAU proposed to set in the ECs. While he was confident the CAU analysts could identify logical investigative steps, he thought they should nevertheless coordinate with the operational personnel to see if there was agreement and to determine whether a lead potentially could affect any ongoing operations that the CAU was not aware of. He also noted that his CAU Unit Chief successors discontinued this practice, a decision he disagreed with and complained about to the Section Chief for CXS because he believed the program risked losing a measure of effectiveness and efficiency as a consequence. ~~(S//NF)~~

Another step the CAU Unit Chief took relating to the FBI's management of Stellar Wind information was to open an administrative file, or "control file," to serve as the repository for all communications that the CAU sent to the field offices containing Stellar Wind information, as well as all communications the CAU received from field offices reporting the results of the investigative activity taken in response to assigned leads.[106] As explained previously, the [redacted] communications had been b1, b3, b7E

[redacted]

disseminated from a subfile associated with the FBI's international terrorism investigation of the September 11 attacks. In the EC requesting that a control file be opened for Stellar Wind information, the CAU Unit Chief wrote that "a dedicated control file for this project will better serve the specific needs of the special project and will add an additional layer of security for the source." ~~(TS//STLW//SI//OC/NF)~~

A control file for Stellar Wind information was opened on September 30, 2002, and given the designation [redacted] From that point forward, all ECs that disseminated Stellar Wind tips were sent in connection with the [redacted] control file.[107] The ECs were classified at the Secret level and, similar to the [redacted] ECs, included a vague explanation about the source of the information and a caveat concerning its use.[108] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

[107] The Unit Chief told us that Director Mueller held a telephone conference call in October 2002 with the heads of all FBI field offices and advised them that FBI Headquarters was working to improve the process for disseminating [redacted] information to the field offices by adding both context and clarity to the communications. Director Mueller expressed his expectation that the offices would act on the information. According to the Unit Chief, Director Mueller essentially was trying to sell the program and ensure the "tool" was being used. Director Mueller told the OIG that he did not recall having specific discussions with the heads of FBI field offices about Stellar Wind information. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

[redacted] b1, b3, b7E

Several months later, in January 2003, the CAU Unit Chief sent an EC to all FBI field offices seeking "to clarify the mission of [CAU] . . . as well as to describe this unit's distinct role in the FBI's participation in the global war on terror." The EC emphasized CAU's capabilities in examining telephone calling activity and its liaison function with members of the U.S. Intelligence Community that are "in a unique position to provide potentially actionable intelligence to the FBI." The EC explained that many of the leads from the CAU were sent under the [redacted] file. On the subject of investigative responses to [redacted] leads, the EC stated: b1, b3, b7E

[redacted] b1, b3, b7E

C. FBI Assigns CAU Personnel to NSA on Full-Time Basis ~~(S//NF)~~

The CAU Unit Chief also assigned a team of FBI personnel to the NSA on a full-time basis to manage Stellar Wind information. The Unit Chief told us that shortly before his temporary duty assignment to FBI Headquarters was set to expire, he and the CXS Acting Section Chief briefed Director Mueller's assistant – and later Director Mueller – about the role they recommended that the FBI take in the Stellar Wind program. The CAU Unit Chief recommended co-locating at the NSA approximately four FBI agents and analysts with remote access to FBI information systems. He likened the suggestion to a "task force environment" that would introduce the FBI's investigative skills at the beginning of the NSA's analysis of Stellar Wind information. Director Mueller approved the recommendation and told the CAU Unit Chief to implement it. ~~(S//NF)~~

For the next 2 months, the CAU Unit Chief worked with the NSA on the proposal. [redacted] b1, b3, b7E

[redacted] The Memorandum of Understanding between the FBI and the NSA to facilitate the co-location was finalized in December 2002, and in February 2003 a CAU team began its co-location at the NSA to manage the FBI's involvement in Stellar Wind. This co-location continues today. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

VI. OIG Analysis (U)

In analyzing the Department's and the FBI's involvement in the NSA's expanded signals intelligence collection activity after the September 11 attacks, it is important to recognize the exceptional circumstances that existed at the time. Many Department and FBI officials emphasized to us the sense of crisis and alarm during this period, and noted the widely shared concern within the Intelligence Community that a second wave of attacks was imminent. The Stellar Wind program was conceived and implemented amid these challenging circumstances. ~~(S//NF)~~

This chapter described the role of Justice Department and FBI officials in the inception and early implementation of the Stellar Wind program, including the Department's initial reviews of the legality of the program. ~~(TS//SI//NF)~~

We believe that a significant problem during this early phase of the Stellar Wind program was the lack of a sufficient number of Justice Department attorneys read into the program to conduct an analysis of the program's legality. The White House – and according to Gonzales, the President – determined who within the Department was permitted access to the program. We believe that Attorney General Ashcroft, who met frequently with the President on national security matters, was in a position to personally advocate for the read-in of an adequate number of attorneys necessary for the Department to perform a thorough and factually accurate legal analysis of the program. We know that Ashcroft's request that his chief of staff David Ayres and Deputy Attorney General Larry Thompson be read into the program was not granted. But because Ashcroft did not agree to be interviewed, we were unable to determine from him whether he sought additional Department read-ins to assist in the legal analysis of the program, how hard he may have pressed for these additional resources, or whether he believed he was receiving adequate legal advice about the program from Yoo alone. ~~(TS//SI//NF)~~

As described in this chapter, John Yoo was the only Department attorney read in to work on the legal analysis supporting the program from

September 2001 through May 2003.[109] As described in Chapter Four, Department officials who succeeded Yoo concluded that the analysis Yoo produced was significantly flawed and found the legal basis for aspects of the program to be lacking. We believe that reading in only one Department attorney to analyze the legality of the program impeded the Department's ability to conduct a thorough and factually accurate legal analysis, and undermined the Department's early role in the program. In Chapter Four we discuss the harm that resulted in late 2003 and early 2004 from the Department's highly restricted access to the program. ~~(TS//SI//NF)~~

We also described in this chapter how the harm attributable to the Justice Department's insufficient early involvement in the program extended beyond conducting an analysis of the program's legality. The Justice Department's relationship with the FISA Court was put at risk by not having officials from OIPR and members of the FISA Court read into Stellar Wind when program-derived information started being disseminated as investigative leads to FBI field offices. In our view, it was foreseeable that Stellar Wind-derived information would be included in FISA applications.[110] OIPR Counsel Baker told us that the Department's counterterrorism and counterintelligence efforts rely on good relations with the FISA Court and that candor and transparency are critical components of the relationship. Baker attributed the Department's record of success with FISA applications and the improved coordination between intelligence agents and prosecutors to the strong relationship that the Department built with the Court. Baker believed, and we agree, that it would have been detrimental to the relationship if the Court learned that information from Stellar Wind was

---

[109] As was the case with Ashcroft, because Yoo did not agree to be interviewed we were unable to learn from him what if any efforts he made either within the Department or at the White House to advocate for additional attorneys – including his supervisor in OLC – to be read into the program to assist in his legal analysis. However, in his book "War by Other Means," Yoo wrote of his experience working on the Stellar Wind program:

> While meeting with Ashcroft alone reflected the importance of the issues, it also placed me in a difficult position. I could not discuss certain matters with my DOJ superiors, or rely on the collective resources of OLC, which usually assigned several attorneys to work on an opinion. Operational security demanded by the war on terrorism changed some of OLC's standard operating procedures.

War by Other Means at 101. ~~(S//NF)~~

[110] The restrictions the FBI imposed on the use of program-derived information – that it could be used for "lead purposes" only and not for "legal or judicial purposes" (such as affidavits) – reflected a good faith and reasonable effort. However, such restrictions could not ensure that program-derived information would not appear in FISA applications. Indeed, this eventuality led to Baker's discovery of the program. ~~(TS//STLW//SI//OC/NF)~~

included in FISA applications without the Court being told so in advance. ~~(TS//STLW//SI//OC/NF)~~

Yet we are not aware of any effort or consideration on the part of Attorney General Ashcroft or officials at the White House to account for Stellar Wind's impact on Justice Department FISA operations by reading in any OIPR officials or members of the FISA Court. In fact, as we described in this chapter, Baker was read into Stellar Wind only after hearing from an FBI colleague that "there is something spooky going on" with the collection of foreign-to-U.S. communications and subsequently reviewing a FISA application that contained "strange, unattributed" language that the FBI would not explain to him. Baker was read in when Daniel Levin, then Counselor to Ashcroft and Chief of Staff to Mueller, pressed White House officials for the clearance. ~~(TS//STLW//SI//OC/NF)~~

Moreover, White House officials initially rejected the idea of reading in members of the FISA Court, and then took no action even as Levin, who together with Ashcroft agreed with Baker that the Court needed to be informed about the program, continued to press the issue. It was not until Levin was required to sign and file a FISA application that Baker refused to handle because it contained Stellar Wind-derived information that the decision was made to read in a single judge (Presiding Judge Lamberth, followed by Presiding Judge Kollar-Kotelly). ~~(TS//STLW//SI//OC/NF)~~

The decisions to read in Baker and a member of the FISA Court, which in our view were unnecessarily delayed, were important steps in preserving the relationship the Justice Department had built with the Court. However, we believe that once Stellar Wind's impact on the Justice Department's FISA operations became evident, limiting read-ins to a single OIPR official and a single FISA Court judge was unduly restrictive and short-sighted. This chapter described how the scrubbing procedures imposed by the FISA Court and implemented by OIPR to account for Stellar Wind-derived information created concerns among some OIPR attorneys about the unexplained changes being made to their FISA applications. The scrubbing procedures also substantially distorted the assignment of cases to FISA Court judges and by November 2004 resulted in Judge Kollar-Kotelly handling approximately [redacted] percent of all FISA applications. In our view, once Stellar Wind began to affect the functioning of the FISA process, OIPR and the FISA Court effectively became part of the program's operations and the number of OIPR staff and FISA Court judges read into Stellar Wind to manage the impact should have increased. ~~(TS//STLW//SI//OC/NF)~~

This chapter also described the FBI's handling of Stellar Wind-derived information in the initial weeks and months of the program. The FBI's chief objective during this period was to expeditiously disseminate

program-derived information to FBI field offices for investigation while protecting the source of the information and the method by which it was obtained. We concluded that the FBI's procedures to meet this objective generally were reasonable. The FBI personnel assigned to the [redacted] developed a straightforward process for receiving Stellar Wind reports, reproducing the information in a non-compartmented, Secret-level format, and disseminating the information in Electronic Communications, or ECs, to the appropriate field offices for investigation. The [redacted] ECs disseminated to FBI field offices also placed appropriate restrictions on how the information could be used, instructing field offices that the information was "for lead purposes only" and could not be used for any legal or judicial purpose. FBI personnel at the field offices we visited as part of our review generally were familiar with the restrictions. ~~(S//NF)~~ b1, b3, b7E

However, we found that the exceptionally compartmented nature of Stellar Wind created deficiencies in the FBI's initial process for handling program-derived information and understandably frustrated agents assigned to handle [redacted] leads. The limited resources allocated to the [redacted] hampered the analysts' ability to enhance Stellar Wind information with relevant FBI or public source information before disseminating leads to field offices for investigation. More significantly, the [redacted] was prohibited from disclosing information that agents traditionally were accustomed to receiving with leads that required investigation. The [redacted] ECs consequently suffered from vagueness about the source of the information being provided and lacked factual details about the individuals allegedly involved with international terrorism and with whom the domestic numbers being disseminated possibly were in contact. ~~(S//NF)~~ b1, b3, b7E

We found that the FBI sought over time to address these deficiencies and improve the effectiveness of its participation in the Stellar Wind program. In April 2002, transmitting Stellar Wind-derived leads to FBI field offices became a priority of the Communications Exploitation Section, and within it, the Communications Analysis Unit (CAU). The first chief of the CAU assigned a team of FBI personnel to work full-time at the NSA on Stellar Wind and to initiate the [redacted] project to manage the FBI's participation in Stellar Wind. As we discuss in this chapter and in Chapter Six, these measures enhanced the FBI's knowledge about Stellar Wind operations and gave the NSA better insight about how FBI field offices investigated Stellar Wind information, which improved Stellar Wind reports and the leads that were disseminated to FBI field offices. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

CHAPTER FOUR
LEGAL REASSESSMENT OF STELLAR WIND (MAY 2003 THROUGH MAY 2004) ~~(TS//SI//NF)~~

By early 2003, while the operation of the Stellar Wind program had evolved, particularly with respect to the means by which intelligence from the program was provided to the FBI, the program still remained legally premised on John Yoo's November 2001 and October 2002 Office of Legal Counsel memoranda. ~~(TS//SI//NF)~~

This chapter describes the pivotal period between May 2003 and May 2004 during which Yoo's departure from the Office of Legal Counsel and the arrival of new officials at the Justice Department resulted in a comprehensive reassessment of the Stellar Wind program's legal basis. This legal reassessment led to a contentious dispute between the Justice Department and the White House on the legality of important aspects of the program. This dispute eventually resulted in modifications to the operation of the program, and also contributed to the decision to place at least one aspect of the program under FISA authority. ~~(TS//STLW//SI//OC/NF)~~

Section I of this chapter discusses how personnel changes within the Office of Legal Counsel led to a re-examination of Yoo's legal analysis, culminating in a Justice Department legal position against continuing to certify the program and the resulting dispute with the White House. Section II describes how, faced with the prospect that the Attorney General, Deputy Attorney General, FBI Director, and other senior Department officials would resign in March 2004 if the program continued unchanged, the White House agreed to modify the program to conform it to the Department's revised legal analysis. ~~(TS//SI//NF)~~

I. Justice Department Reassesses Legality of Stellar Wind Program ~~(TS//SI//NF)~~

A. Overview of Office of Legal Counsel (U)

One of the responsibilities of the Assistant Attorney General for the Office of Legal Counsel (OLC) is to assist the Attorney General in his function as legal advisor to the President and all Executive Branch agencies. OLC drafts legal opinions for the Attorney General and also provides its own opinions in response to requests from the Counsel to the President, various agencies of the Executive Branch, and offices within the Department of Justice. OLC often deals with complex legal issues on which two or more agencies are in disagreement, and provides legal advice to the Executive Branch on constitutional questions, including the review of pending

legislation for constitutionality. Executive Orders proposed to be issued by the President are reviewed by OLC as to form and legality, as are other matters that require the President's formal approval. OLC also reviews proposed orders by the Attorney General and all regulations requiring the Attorney General's approval. (U)

B. Personnel Changes within Office of Legal Counsel (U)

John Yoo advised Attorney General Ashcroft and White House officials on the Stellar Wind program from the program's inception in October 2001 through Yoo's resignation from the Department in May 2003. Upon Yoo's departure, Patrick Philbin told the OIG that he was selected by the White House to assume Yoo's role as advisor to the Attorney General concerning the program.[111] With this personnel change came a fresh review of the legal underpinnings of the Stellar Wind program. We describe in the following sections the circumstances leading to what one official described as "the great rethink" of the program. ~~(TS//SI//NF)~~

1. Yoo's Role in the Program (October 2001 through May 2003) (U)

On September 11, 2001, and through November 2001, Daniel Koffsky was the Acting Assistant Attorney General for OLC. Koffsky was not read into the Stellar Wind program. Jay Bybee served as Assistant Attorney General for OLC from November 2001 until March 2003, when he became a judge on the U.S. Court of Appeals for the Ninth Circuit.[112] Bybee also was never read into the Stellar Wind program. As discussed in Chapter Three, John Yoo, a Deputy Assistant Attorney General in OLC, had sole responsibility within that office and within the Department of Justice for developing the legal analysis relating to the Stellar Wind program until May 2003.[113] Bybee told us he was not aware at the time that Yoo was drafting legal opinions in connection with a compartmented program. ~~(TS//SI//NF)~~

Bybee told us that the OLC normally adheres to a tradition called the "two Deputy rule," so that OLC opinions are reviewed by two OLC Deputy Assistant Attorneys General before going to the OLC Assistant Attorney General for approval. Bybee said that the purpose of this rule is to ensure

---

[111] On June 1, 2003, Philbin became an Associate Deputy Attorney General. However, he told us that he still technically remained a Deputy Assistant Attorney General in OLC and was thus "dual-hatted." (U)

[112] Bybee was nominated by President Bush to serve on the Ninth Circuit in May 2002 but was not confirmed by the Senate until March 2003. (U)

[113] Yoo's major opinions about electronic surveillance and Stellar Wind are summarized in Chapter Three. ~~(TS//SI//NF)~~

the quality of the legal research and soundness of the legal analysis. In addition, Bybee stressed that the Assistant Attorney General must be aware of all opinions that issue from the OLC. Bybee said that the OLC Assistant Attorney General has an obligation to "see the whole picture" and is the only person in the office who knows the full range of issues that are being addressed by the OLC. Bybee also said the Assistant Attorney General is the only official in that office who can assure that OLC opinions remain consistent. Bybee stated that the Assistant Attorney General, as a Senate-confirmed official, has ultimate accountability for the work of the office. Bybee noted that, by contrast, the Deputy Assistant Attorney General position, though political, does not require Senate confirmation. (U)

Bybee told the OIG that it would not be unusual for a Deputy Assistant Attorney General such as Yoo to have direct contact with the White House for the purpose of rendering legal advice. Bybee stated that it is "not clear" whether or to what extent the Attorney General needs to be kept informed of such contacts. However, Bybee said that the Attorney General may appropriately decide to ask a single OLC attorney to work on a particular project, but that it is "not the White House's call" to make such assignments because the White House may not be aware of what advice the OLC is providing to other Executive Branch agencies. Bybee told us that during his tenure as Assistant Attorney General he did not know that Yoo was working alone on a sensitive compartmented program, and he had no knowledge of how Yoo came to be selected for this responsibility. (U)

Philbin said he believed that White House Counsel Gonzales and Vice President Cheney's Counsel David Addington had selected Yoo to draft the OLC's opinions on Stellar Wind and other national security programs, and that Yoo was the "obvious choice" to assume this role because of his expertise in war powers issues and the authority of the Commander-in-Chief.[114] ~~(S//NF)~~

Gonzales told the OIG he understood that Yoo had asked others within OLC to help out with specific legal issues during this period without telling them what they were being asked to assist with, and Yoo then aggregated that work into his memoranda concerning electronic surveillance and the Stellar Wind program. Gonzales also stated that Yoo did not consult with any experts outside the Department in drafting his memoranda.[115] ~~(TS//SI//NF)~~

---

[114] As discussed in Chapter Three, Yoo had been given responsibility for working on national security issues prior to the inception of the Stellar Wind program. (U)

[115] When Gonzales testified before the Senate Judiciary Committee on February 6, 2006, he stated that although he was not at the Department when the program commenced, "I suspect – in fact I'm fairly sure – that there were not discussions with (Cont'd.)

As noted above, neither Yoo nor Ashcroft agreed to be interviewed for the OIG's investigation. Other witnesses gave the OIG various accounts of Yoo's interactions with Attorney General Ashcroft and with the White House concerning the program. Gonzales told us that Yoo regularly advised Ashcroft on the legal aspects of the program so that Ashcroft could continue to certify it as to form and legality. Gonzales also said that it was incumbent on Ashcroft as Attorney General to satisfy the Department's legal obligations regarding the program. Gonzales told us he thus understood Yoo's opinions as representing the opinions of the Department. However, Gonzales acknowledged that White House officials consulted with Yoo and sought his advice without going through the Attorney General or Bybee – Yoo's supervisor – although Gonzales also said they did not seek Department approval from Yoo concerning the Stellar Wind program. ~~(TS//SI//NF)~~

Other witnesses described their concerns regarding Yoo's direct contacts with the White House, and with Addington and Gonzales in particular. Philbin said he told Addington that Yoo's direct access to Addington on legal matters was "not a good way to run things," referring to the lack of oversight of an OLC Deputy Assistant Attorney General by a supervisor. Philbin stated that there was nothing wrong with assigning a project to a subordinate, but not without the head of the office knowing what the subordinate was doing. (U)

Jack Goldsmith told us that when he became the Assistant Attorney General for the Office of Legal Counsel in October 2003, he learned that Yoo's contacts with the White House had had the effect of cutting the Attorney General "out of the loop," a practice Goldsmith said he resolved not to continue with any OLC attorney. (U)

Goldsmith also told us the White House had wanted Yoo to replace Bybee as the Assistant Attorney General for the Office of Legal Counsel following Bybee's confirmation as a judge on the Ninth Circuit, but that Ashcroft blocked the move. Yoo resigned from the Department in May 2003.[116] (U)

---

outside expertise at the Department, although I don't know for sure." An NSA Associate General Counsel for Operations told the OIG that Yoo visited the NSA for a briefing about the program at some point after he had drafted his November 2, 2001, legal memorandum. ~~(TS//SI//NF)~~

[116] In addition to working on the legal analysis for the Stellar Wind program while at the Justice Department, Yoo also worked on at least one other project involving a Top Secret compartmented detainee interrogation program. In contrast to the Stellar Wind program, the OIG determined that at least three OLC attorneys, including Bybee and Philbin, worked on the program's legal analysis with Yoo or participated by supervising his work. In addition, attorneys from the Department's Criminal Division and from other

(Cont'd.)

2. Philbin Replaces Yoo (U)

Patrick Philbin joined the Department as a Deputy Assistant Attorney General in the Office of Legal Counsel on September 4, 2001.[117] He was read into the Stellar Wind program in late May 2003, just before Yoo left the Department. Philbin said that he, accompanied by Yoo, was read into the program by Addington in Addington's office in the Old Executive Office Building. Philbin told us that Addington provided an overview of the program, describing the two basic categories of collection as "content" and "meta data." Philbin said that later, based on his legal analysis of the Stellar Wind program, he developed the "three baskets" terminology to describe more specifically the three types of collections. ~~(TS//STLW//SI//OC/NF)~~

Philbin said he was told by Addington he was being read into the program because Yoo was leaving the Department and another attorney was needed to review the threat assessments that supported the Presidential Authorizations and to then advise the Attorney General on recertifying the program as to form and legality.[118] Philbin said he also was told that he and the Attorney General were the only Justice Department officials who were supposed to be involved in this "review and recertification" process. Philbin told us he was aware that OIPR Counsel James Baker had also been read into the program; however, Philbin stated that Addington told him he should not discuss the program with Baker and should only advise the Attorney General on the program. Philbin said he believed Addington did not want Philbin speaking with Baker about the program because Addington had always taken the position that the program should be kept as compartmented as possible.[119] ~~(TS//SI//NF)~~

---

agencies were regularly consulted by Yoo in his drafting of the legal memoranda on the legality of this program. Yoo told the Department's Office of Professional Responsibility that Attorney General Ashcroft determined who was allowed to work on the memoranda for the detainee interrogation program. Transcript of Interview of John Yoo by Office of Professional Responsibility, June 7, 2005, at 12. ~~(TS//STLW//SI//OC/NF)~~

[117] Prior to joining the Department Philbin had been at a private law firm and had specialized in telecommunications law. (U)

[118] When asked whether he had any knowledge of the program prior to being read in, Philbin said he did not, but he recalled that in the fall of 2001 he had a discussion with Yoo about some general electronic surveillance issues. Yoo told Philbin that Yoo was told to work alone on this particular matter. Yoo did not state who had given him this instruction. ~~(TS//SI//NF)~~

[119] Baker told us he was not similarly advised to avoid discussions with Philbin about the program, nor was he aware that Addington had instructed Philbin not to discuss the program with him. In fact, according to Baker, Philbin initiated several conversations with Baker about the operational details of the program as Baker understood them at the time. (U)

The day after being read into the program, Philbin moved from the Office of Legal Counsel to the Office of the Deputy Attorney General to become an Associate Deputy Attorney General, although technically he still retained his OLC Deputy Assistant Attorney General position and was thus "dual-hatted." Philbin took over the "national security portfolio" from David Kris, who had recently left the Department. Philbin stated he was "somewhat concerned" that he would be advising the Attorney General on the Stellar Wind program even though Deputy Attorney General Larry Thompson, Philbin's supervisor, was not read into the program. However, Philbin said he anticipated at the outset that his work on the program would not require a lot of his time. ~~(S//NF)~~

3. Initial Concerns with Yoo's Analysis (U)

Philbin said that after he was read into the Stellar Wind program he believed he needed to do "due diligence" to learn about the program. He said he reviewed Yoo's legal opinions about the program and realized that Yoo had omitted from his analysis any reference to the FISA provision allowing the interception of electronic communications without a warrant for a period of 15 days following a congressional declaration of war. See 50 U.S.C. § 1811. Philbin also stated that Yoo's OLC opinions were premised on the assumption that FISA did not expressly apply to wartime operations, an assumption that from Philbin's perspective rendered the opinions "problematic." Philbin said that this gap in Yoo's analysis was his first indication that the legal reasoning underpinning the Presidential Authorizations would have to be revisited. ~~(TS//STLW//SI//OC/NF)~~

Philbin said the second indication of problems with Yoo's analysis came when he read a summary document Yoo had prepared concerning the program.

(b)(3), (b)(7), (b)(3)

(b) (5)

~~(TS//STLW//SI//OC/NF)~~

Second, and more significantly, Philbin stated that

(b) (5)

~~(TS//STLW//SI//OC/NF)~~

(b) (5)

(b) (5)

(b) (5)

~~(TS//STLW//SI//OC/NF)~~

(b) (5), (b)(1), (b)(3)

[120] See Presidential Authorization of April 22, 2003 at para. 4(b)(i) & (ii). The April 22, 2003, Authorization was the only Authorization personally approved as to form and legality by Yoo. He approved the Authorization on April 18, 2003, five days before the date of his talking points memorandum. ~~(TS//STLW//SI//OC/NF)~~

[121] In fact, as discussed in Chapter Five, the reasonable articulable suspicion standard was the only standard the government sought to apply to its authority to query the e-mail meta data collection after basket 3 of Stellar Wind was placed under FISA authority in July 2004. ~~(TS//STLW//SI//OC/NF)~~

(b) (5)

(b) (5), (b)(1), (b)(3)

Philbin said the errors in the Yoo's talking points document represented "a significant step toward the realization that the whole legal analysis was screwed up." Philbin told us he felt he could not rely on the existing analysis and that he needed to "build from the ground up." ~~(TS//SI//NF)~~

4. Problems with (b)(1), (b)(3) ~~(TS//STLW//SI//OC/NF)~~

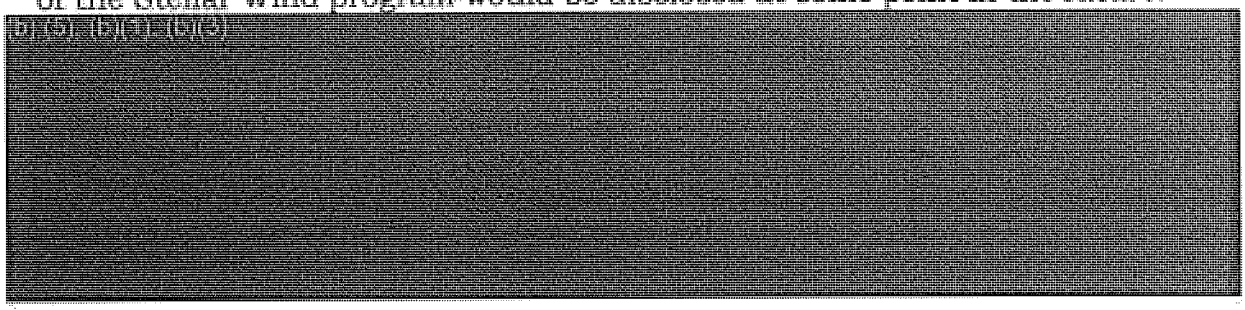
In addition to the flaws Philbin identified in Yoo's legal analysis, Philbin told us he grew increasingly concerned that

(b) (5), (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~

[122] Philbin told us he visited the NSA three times during the summer of 2003 in an effort to learn how the program operated. Several officials we interviewed told us that Philbin understood the program well, in part due to his background in telecommunications law. (U//~~FOUO~~)

Philbin said that he and later Goldsmith recognized that the existence of the Stellar Wind program would be disclosed at some point in the future.



(b) (5), (b)(1), (b)(3)

(TS//STLW//SI//OC/NF)

5. Other Collection Concerns (S//NF)

Philbin told us that during the summer of 2003 he identified other concerns about the Stellar Wind program. First, Philbin said he began to believe that the existing OLC memoranda failed to describe the (b)(5), (b)(1), (b)(3)

Philbin said he also had concerns over (b) (5), (b)(1), (b)(3)

(TS//STLW//SI//OC/NF)

6. Decision to Draft New OLC Memorandum (U)

In August 2003, Philbin brought his concerns about the OLC legal opinions to Attorney General Ashcroft. Philbin told Ashcroft that there were problems with the legal analysis supporting the program but probably not with the conclusions reached. Philbin told us that he believed that since the conclusions would not change there would be no need to "pull the plug" on the analytically problematic aspects of the program. Philbin said he

---

[123] As described later in this chapter, the term "acquired" was not clarified until the March 11, 2004, Presidential Authorization. That Authorization stated that meta data was "'acquired' . . . when, and only when, the Department of Defense has searched for and retrieved such header/router/addressing-type information, including telecommunications dialing-type data (and not when the Department obtains such header/router/addressing-type information, including telecommunications dialing-type data, such as (b)(1), (b)(3) for retention)."

(b)(3), (b)(1)

(TS//STLW//SI//OC/NF)

[124] (b) (5), (b)(1), (b)(3)

(TS//STLW//SI//OC/NF)

therefore advised that Ashcroft could continue to certify the program "as to form and legality." ~~(TS//SI//NF)~~

However, Philbin also recommended that a new OLC memorandum be drafted. According to Philbin, Ashcroft concurred, told him to continue working on his analysis, and asked to be kept updated on Philbin's progress. After meeting with Ashcroft to discuss the issue, Philbin said he began to write a new memorandum on the legality of the entire Stellar Wind program.[125] ~~(TS//SI//NF)~~

C. Reassessment of Legal Rationale for the Program ~~(TS//SI//NF)~~

1. Goldsmith Becomes OLC Assistant Attorney General (U)

Jack Goldsmith told the OIG that he was recommended for the Assistant Attorney General position by Yoo after Yoo was not selected for the position. Goldsmith stated that during his interview for the position, Attorney General Ashcroft and Ashcroft's Chief of Staff David Ayres emphasized that the OLC Assistant Attorney General must keep the Attorney General informed of matters the Office of Legal Counsel was working on and stressed the importance of keeping the Attorney General "in the loop." Goldsmith told the OIG that he believed Ashcroft and Ayres raised these issues as a result of their experience with Yoo. (U)

Goldsmith was selected for the position, confirmed by the Senate, and on October 6, 2003, was sworn in as the OLC Assistant Attorney General. (U)

According to Goldsmith, he was told by Department colleagues that the procedures OLC historically followed in drafting its opinions were changing and that the Attorney General was being circumvented in the new

---

[125] Philbin said that he was not certain at the time that Ashcroft fully understood the (b)(1), (b)(3) because the subject matter was "difficult." Philbin also stated that for "client management" purposes, he needed to first make sure that he too fully understood the issues before raising his concerns to others. He said he did not just want to be "a naysayer" identifying problems, but also wanted to propose solutions. He said that the program would be examined by Congress one day and that the legal analysis had to be "carefully done to protect the President." Philbin said he therefore believed that the OLC legal memoranda had to be rewritten to achieve that objective. Philbin told us he also was concerned that the program not appear like a "rogue operation," but rather as a responsible approach to collecting intelligence with adequate controls and oversight. In this regard, Philbin emphasized that it would be important to demonstrate that the program had appropriate restrictions based on the law, and that the restrictions guarded against abuses. ~~(TS//SI//NF)~~

process. Goldsmith said that OLC Principal Deputy Assistant Attorney General Ed Whelan also told him that OLC's procedures, built on custom and practice but still "hugely important," had "broken down" prior to Goldsmith's arrival as the Assistant Attorney General. (U)

Goldsmith told us that he also became aware that Ashcroft sensed there was a White House-Office of Legal Counsel relationship over which Ashcroft did not have full control. Goldsmith said that when he became the OLC Assistant Attorney General he immediately moved to "bring things back to normalcy" by, for example, making sure all OLC memoranda were provided to client agencies for review and input and that all memoranda were reviewed by two OLC deputies, as was the traditional OLC practice.[126] (U)

With regard to the Stellar Wind program, Philbin told us he had always intended to request that Goldsmith be read into the program after Goldsmith was confirmed by the Senate. Philbin said that he went to the White House and asked Addington (and possibly Gonzales) to have Goldsmith read into the program. Philbin stated that Addington told him that he would have been "fine" with not allowing Goldsmith to be read in, and that Philbin would have to justify the request before Addington would convey the request to the President. Philbin told us he explained to Addington that he would need to have the head of OLC sign off on the new memorandum he was writing or the memorandum would lack credibility. (U//~~FOUO~~)

On November 17, 2003, Goldsmith was read into the Stellar Wind program by Addington in Addington's office.[127] Philbin was also present. On the way to the read-in, Philbin told Goldsmith to "prepare for your mind to be blown." Goldsmith told us that the read-in took approximately 5 minutes, and when it was over he remarked to Philbin, "That doesn't seem

---

[126] Goldsmith's view of how the OLC should operate was later echoed by a subsequent head of the office, Steven Bradbury. In a May 16, 2005, internal OLC guidance memorandum entitled "Best Practices for OLC Opinions," Bradbury emphasized that OLC legal memoranda should reflect the positions and expertise of interested agencies, and he also stressed the importance of a rigorous peer review process within the office before finalizing OLC memoranda. (U)

[127] After Ashcroft, Yoo, Baker, and Philbin, Goldsmith was only the fifth non-FBI Justice Department official to be read into the Stellar Wind program since the program's inception over 2 years earlier. Philbin stated that prior to Goldsmith's arrival at the Department and subsequent read-in to the program, he had no one to help him draft a new legal memorandum and no one other than Ashcroft with whom to discuss the legal issues. He told the OIG that it was extremely beneficial to have another attorney working with him on the project. Philbin also told us he did not press the White House to read in additional attorneys during the summer 2003 period before Goldsmith arrived at the Department. ~~(TS//SI//NF)~~

so bad." Goldsmith said that 3 weeks later, after studying the matter, he would come to a "different conclusion." (U//~~FOUO~~)

2. NSA Denied Access to OLC Memoranda (U//~~FOUO~~)

One of the first Stellar Wind meetings Goldsmith and Philbin attended after Goldsmith's read-in was held in the DOJ Command Center with Addington, NSA Deputy General Counsel Vito Potenza, and NSA Inspector General Joel Brenner. Goldsmith stated that the NSA Inspector General requested a copy of the OLC legal memoranda regarding the program as part of an audit the NSA Office of the Inspector General wanted to conduct of the program. According to Goldsmith, Addington "bit [the Inspector General's] head off," and made it clear that the memoranda would not be provided to the NSA OIG. (~~TS//SI//NF~~)

Goldsmith said he learned either at that meeting or shortly thereafter that NSA's Office of General Counsel also had been denied access to the OLC memoranda. Bob Deitz, the NSA General Counsel during this period, told the NSA OIG that he was never permitted to see Yoo's legal memoranda. Dietz stated that he called Addington several weeks after the first Presidential Authorization was signed and asked if he could see a copy of Yoo's memorandum (likely the November 2, 2001, memorandum), and that Addington responded "no." Dietz said that Addington would only read "a paragraph or two" from the memorandum to him over a classified telephone line. Deitz stated that he never advised Yoo on his legal analysis, although he did advise NSA Director Hayden that he thought the program was legal and within the President's authority. (~~TS//SI//NF~~)

The OIG also interviewed (b)(6), (b)(3) the NSA's Associate General Counsel for Operations during Yoo's and Goldsmith's tenure in OLC.
b3, b6 (b)(3), (b) told us that he was not troubled by the fact that other senior NSA officials had been denied access to Yoo's legal memoranda, and that he felt no need to review them. (b)(3), (b) stated that his primary concern with respect to the legality of the program was whether "Justice was comfortable with it." (b)(3), (b) also stated that he assumed that the Justice Department would find the program legal by resolving the tension between FISA and the President's inherent Commander-in-Chief authority based upon the doctrine of constitutional avoidance. (~~TS//STLW//SI//OC/NF~~)

Goldsmith told us he found it "shocking" that the NSA was not provided access to Yoo's legal memoranda. He stated that the decision to withhold the memoranda was one of the "most astonishing things" he learned about how the program was handled, and that he could not "draw a good inference" from that fact. Goldsmith emphasized that under the Stellar Wind program the NSA had been asked to do something contrary to its ordinary practices, and yet was not allowed to review the legal

justifications for being permitted to do it. Goldsmith told us he believed that the NSA might have identified problems or mistakes in Yoo's analysis early in the program had it been given access to his memoranda. ~~(TS//SI//NF)~~

Goldsmith told us that upon becoming the Assistant Attorney General he intended to reverse the practice of keeping OLC memoranda closely held, and that he also decided he would seek client agency expertise in drafting these documents. (U)

3. Goldsmith Joins Effort to Reassess Legal Basis for the Program ~~(TS//SI//NF)~~

In the two or three weeks following his read-in to the Stellar Wind program, Goldsmith reviewed several documents to educate himself about the program. These included the memorandum that Philbin had already begun to draft (which included a description of how the program worked operationally), Yoo's memoranda, and older OLC memoranda concerning surveillance activities. After Goldsmith familiarized himself with the program, Goldsmith provided Philbin with additional research and helped supplement Philbin's draft memorandum. ~~(TS//STLW//SI//OC/NF)~~

Goldsmith stated that Philbin had done an "amazingly heroic job" in reviewing the program. Goldsmith believed "ninety-nine out of a hundred" attorneys in Philbin's position, having been asked simply to opine as to form and legality, would have just relied on the previous Office of Legal Counsel memoranda. Goldsmith said that Philbin, however, was not convinced by those memoranda and therefore did not rely on them. In addition, Goldsmith noted that Philbin sought to understand the program as it was actually implemented at the NSA before advising the Attorney General on its legality. ~~(TS//SI//NF)~~

(b)(1), (b)(3), (b) (5)

[redacted]

128

(b)(1), (b)(3), (b) (5)

[redacted]

(Cont'd.)

(b) (5)

[redacted]

~~(TS//STLW//SI//OC/NF)~~

4. AUMF Becomes the Primary Legal Rationale Supporting (b)(1)/(b)(3) of the Stellar Wind Program ~~(TS//STLW//SI//OC/NF)~~

(b) (5); (b)(1); (b)(3)

[redacted]

Goldsmith concluded the NSA's interception of (b)(1)/(b)(3) did not comply with FISA's requirement to obtain judicial authorization, and did not fall within any of the exceptions to this requirement. Goldsmith later wrote in his legal memorandum reassessing the legality of the program that a proper analysis

(b) (5)

[redacted] ~~(TS//STLW//SI//OC/NF)~~

139

(b) (5)

[redacted]

139 See Goldsmith's May 6, 2004, memorandum entitled "Review of the Legality of the Stellar Wind Program" (Goldsmith Memorandum, May 6, 2004). This memorandum is discussed in Section II C below. ~~(TS//STLW//SI//OC/NF)~~

of Stellar Wind "must not consider FISA in isolation" but rather must consider whether Congress, by authorizing the use of military force against al Qaeda, also "effectively exempts" such surveillance from FISA. Goldsmith concluded that this reading of the AUMF was correct because the AUMF authorized the President to use "all necessary and appropriate force" against the enemy that attacked the United States on September 11, 2001, and to "prevent any future acts of international terrorism against the United States" by such enemy – authority that has long been recognized to include the use of signals intelligence as a military tool. (~~TS//STLW//SI//OC/NF~~)

Alternatively, Goldsmith reasoned that even if the AUMF did not exempt surveillance under the program from the restrictions imposed by FISA, the question was sufficiently ambiguous to warrant the application of the doctrine of constitutional avoidance, and therefore should be construed not to prohibit the activity.[131] (~~TS//STLW//SI//OC/NF~~)

(b) (5)

[redacted]

(~~TS//STLW//SI//OC/NF~~)

(b) (5), (b)(1), (b)(3)

[redacted]

[131] In his May 6, 2004, memorandum, Goldsmith concluded that if the [redacted] (b)(1), (b)(3) arguments under the AUMF did not create sufficient ambiguity as to trigger the doctrine of constitutional avoidance, FISA as applied would represent an unconstitutional infringement on the President's exclusive authority as Commander-in-Chief in wartime to protect the nation from attack. (~~TS//STLW//SI//OC/NF~~)

[redacted]

5. Office of Legal Counsel Raises its Reassessment of the Stellar Wind Program (December 2003 through January 2004)[133] ~~(TS//SI//NF)~~

During late 2003, Goldsmith and Philbin continued their analysis of the legal bases for the Stellar Wind program. During this time Philbin and Goldsmith were the only two Department officials in a position to brief the Attorney General and White House officials on the status of their legal reassessment and its potential ramifications for the operation of the program.[134] ~~(TS//SI//NF)~~

With the existing Presidential Authorization set to expire on December 11, 2003, Goldsmith and Philbin met with Ashcroft on December 8, 2003, to advise him on recertifying the program as to form and legality. Goldsmith wrote in notes that he maintained during this time period that at the meeting he and Philbin "note[d] problems gently" to Ashcroft. Goldsmith told us Ashcroft was "extraordinarily supportive" of his and Philbin's efforts to reassess the legality of the program and made clear his view that the program had to be on solid legal footing. ~~(TS//STLW//SI//OC/NF)~~

Goldsmith advised Ashcroft that, despite concerns about the program, Ashcroft should certify the December 9, 2003, Authorization. Goldsmith

[redacted]

[133] The narrative in this and the following sections is based on our interviews of Philbin, Goldsmith, Comey, Mueller, Gonzales, and others. We also relied on Philbin's and Goldsmith's contemporaneous notes, Goldsmith's chronology of events that he wrote during this period, Mueller's Program Log documenting events in March 2004, and Attorney General Ashcroft's FBI security detail log of events that occurred while Ashcroft was hospitalized from March 4 through March 14, 2004, among other documents. (U)

[134] James Comey became the Deputy Attorney General on December 9, 2003, but was not read into the program until over 2 months later. (U)

later advised Ashcroft to certify the January 14, 2004, Authorization as well. Goldsmith told us he made these recommendations to Ashcroft with the caveat that although he believed Yoo's memoranda to be flawed, Goldsmith had not yet concluded that the program itself was illegal. ~~(TS//SI//NF)~~

Based on Goldsmith's advice, Ashcroft certified the December 9, 2003, and January 14, 2004, Authorizations. ~~(TS//SI//NF)~~

In December 2003 Philbin and Goldsmith informed Ashcroft that they believed Comey, who was sworn in as the new Deputy Attorney General in December 2003, also needed to be read into the program. Philbin said he justified this request by noting that he would be traveling abroad for 2 weeks later that month on an unrelated Justice Department matter.[135] (U)

In December 2003, Goldsmith and Philbin met with Addington and Gonzales at the White House to express their growing concerns about the legal underpinnings for program. Goldsmith said he told them that OLC was not sure the program could survive in its current form. According to Goldsmith's notes, these discussions did not contemplate an interruption of the program, although the White House represented that it would "agree to pull the plug" if the problems with the program were found to be sufficiently serious. Goldsmith told us that the White House – typically through Addington – told him "several times" that it would halt the program if the Department found that it could not be legally supported. ~~(TS//SI//NF)~~

Philbin told us he recalled that Addington in particular was "annoyed" with the OLC's preliminary conclusion that

(b)(5), (b)(1), (b)(3)

Philbin said that Addington nevertheless told him and Goldsmith to continue analyzing the program and that if serious problems were found, the program would be shut down. ~~(TS//STLW//SI//OC/NF)~~

On December 18, 2003, while Philbin was abroad, Goldsmith met again with Addington and Gonzales. Goldsmith wrote in his chronology that this time he conveyed with "more force" his "serious doubts and the need to get more help to resolve the issue [as soon as possible]." Goldsmith also told Addington and Gonzales that he needed more resources to continue examining the legality of the program. They responded to this request by telling Goldsmith that Philbin should devote all of his time to the project.

---

[135] As discussed in Chapter Three, Comey's predecessor as Deputy Attorney General, Larry Thompson, was never read into the Stellar Wind program despite Ashcroft's request to the White House on behalf of both Thompson and Ashcroft's chief of staff. (U//~~FOUO~~)

Goldsmith told us that he asked to have Comey read into the program. According to Goldsmith's notes, Addington and Gonzales "bristle[d]" at that suggestion. Goldsmith told us he made the request for Comey to be read in because he believed he would need the Deputy Attorney General's assistance to help "make the case" to the White House that the program was legally flawed. Goldsmith also stated that he wanted Comey read in because, as the Deputy Attorney General, Comey was Philbin's direct supervisor. ~~(TS//SI//NF)~~

We asked Gonzales when he first became aware that the Department had concerns about the legality of the Stellar Wind program. Gonzales stated that he remembered that sometime after Philbin and Goldsmith joined the Department, they decided to conduct a programmatic review of the legal basis for Stellar Wind. Gonzales said that he welcomed this review, and that it was always important to reassess the value of or need for the program, as well as its legality. Gonzales told us he thought that Goldsmith and Philbin's review arose out of concerns about Yoo's November 2, 2001, opinion and that their review was limited to that document. Gonzales said that Goldsmith periodically told him that Philbin was reviewing the program and that some questions had been raised or that some changes to the program might be needed as a result of their reassessment. Gonzales said that he told Goldsmith to let him know how the review was progressing. Gonzales also told us he did not recall getting into any specific discussions with Goldsmith about OLC's concerns until early March 2004. ~~(TS//SI//NF)~~

In contrast, Goldsmith told us he had been "crystal clear" with Gonzales and Addington that the Office of Legal Counsel had concerns about the legality of aspects of the program as early as December 2003, although Goldsmith also acknowledged that his discussions with Gonzales and Addington became more detailed in March 2004. Goldsmith told us that he gave the two White House officials the same caveats he gave Ashcroft when advising him on the legality of the program – that there were flaws in Yoo's analysis, but that OLC had not yet concluded that the program itself was illegal. ~~(TS//SI//NF)~~

Goldsmith's efforts to gain the White House's permission to have others (including Comey) read into the program continued through January 2004. According to Goldsmith's notes, both Addington and Gonzales pressed Goldsmith on his reason for the request and continued to express doubt that additional resources were needed. However, in late January the White House agreed to allow Comey to be read in, provided that Philbin devoted all of his time to his analysis of the program and, according to Goldsmith, that the Department's legal analysis be completed by March 2004 when the Presidential Authorization was due to be renewed. (U)

6. Deputy Attorney General Comey is Read into the Program (U)

Comey became the Deputy Attorney General on December 9, 2003, and was read into the Stellar Wind program on February 17, 2004. Comey told us that he had no awareness of the program prior to being read in. He said he learned after his read-in that Addington had resisted Goldsmith and Philbin's efforts to have him read in earlier. Comey said Addington was the "gatekeeper" for Stellar Wind and wanted to keep the program a "close hold." (U)

Comey told us that NSA Director Hayden personally wanted to conduct Comey's read-in to the program. Hayden read in Comey at the Justice Command Center in a briefing that took approximately 20 to 30 minutes. Comey said that, at the read in, Hayden explained the "three baskets" to him. ~~(TS//STLW//SI//OC/NF)~~

Comey told us that after Hayden left the Command Center, Comey and Philbin continued discussing the program. Philbin told Comey that there were problems with the legality of the program and that there were "operational issues" as well. Comey told us that his initial reaction to the program was "unprintable." He said he thought that the NSA could not collect the content of certain communications covered by the program outside of FISA authority. Hayden told the OIG that Comey raised no objections to him about the program upon being read in. (U)

Within the first month after being read in, Comey discussed the program with Ashcroft, Goldsmith, Philbin, and other Department officials who had been read in by this time, including James Baker, Counsel for Intelligence Policy; Chuck Rosenberg, Comey's Chief of Staff, and Daniel Levin, Counsel to the Attorney General.[136] Comey said he did not recall having any discussions about the program with FBI Director Mueller during this period. (U)

Comey also recalled meeting with Scott Muller, the CIA General Counsel, shortly after being read into the program. Comey said that he told Muller about the legal concerns Philbin and Goldsmith had raised regarding Yoo's analysis and that Muller agreed that the concerns were well founded. (U)

Comey also told us that Goldsmith had identified for Comey as a particular concern the notion that Yoo's legal analysis entailed ignoring an

---

[136] Levin had just returned to the Department after working in private practice and serving as a Bush Administration liaison to the September 11 Commission. Rosenberg was read into Stellar Wind in 2003 while serving as Counsel to FBI Director Mueller. (U)

act of Congress, and doing so in secret. Comey stated that Goldsmith described such action as "breathtaking." Comey agreed, describing the action as "unprecedented." (U)

D. Office of Legal Counsel Presents its Conclusions to the White House (U)

On March 1, 2004, Philbin completed a first draft of a revised OLC opinion on the Stellar Wind program. According to Goldsmith's notes, at this time Goldsmith and Philbin had not yet concluded "definitively" that there was "anything certainly wrong" with the program, with the possible exception of the scope of [redacted]
~~(TS//STLW//SI//OC/NF)~~

In explaining the rationale for the revised opinion, Comey described to the OIG his view of two approaches or standards that could be used to undertake legal analysis of government action. If the government is contemplating taking a particular action, OLC's legal analysis will be based on a "best view of the law" standard. However, if the government already is taking the action, the analysis should instead focus on whether reasonable legal arguments can be made to support the continuation of the conduct.[137] Comey said that because Stellar Wind was an ongoing program, Goldsmith and Philbin's analysis proceeded under the second approach. Under this approach, at this point they concluded that there were reasonable legal arguments to be made to continue the collection of [redacted] but they still had not identified a legal argument to support [redacted]
~~(TS//STLW//SI//OC/NF)~~

Comey said that during early March 2004 the sense was that "we can get there" as to [redacted] albeit by using an aggressive legal analysis. However, he said that collection of [redacted] would require [redacted]
[redacted] ~~(TS//STLW//SI//OC/NF)~~

---

[137] Goldsmith emphasized to us that this second situation almost never presents itself, and that OLC rarely is asked to furnish legal advice on an ongoing program because the pressure "to say 'yes' to the President" invariably would result in applying a lower standard of review. Goldsmith stated that OLC's involvement in Stellar Wind was "unprecedented" because OLC is always asked to review the facts and formulate its advice "up front." ~~(S//NF)~~

On March 1, 2004, Comey met with FBI Director Mueller to inform him that the OLC had found problems with the legal authority for the Stellar Wind program, particularly with the [redacted] According to a log Mueller kept documenting events in March 2004 concerning the program, Comey said he was trying to work out these problems with the OLC and "other interested parties."[138] Mueller told us that March 1, 2004, was when he first became aware of the Department's concerns about the legal support for the program. Mueller described the FBI as "recipients of information from the program," and that the dialogue as to the program's legality was between the Department and the White House. ~~(TS//STLW//SI//OC/NF)~~

1. March 4, 2004: Comey Meets with Ashcroft to Discuss Problems with the Program (U)

Comey told us he met with Attorney General Ashcroft for lunch on March 4, 2004, to discuss the Stellar Wind program. Comey reminded Ashcroft of the details of the program and said he used salt and pepper shakers and a knife to represent the three baskets during the discussion. According to Comey, Ashcroft agreed with Comey and OLC's assessment of the potential legal problems, and he instructed Comey to "just fix it" and "tell them to make the changes that need to be done." ~~(TS//STLW//SI//OC/NF)~~

Comey said he assumed Ashcroft meant that Comey should reach out to the NSA and the White House for the necessary changes. The Presidential Authorization in effect at the time was due to expire on March 11, 2004. Comey said Ashcroft did not discuss with him whether he would recertify the program as it was currently being authorized by the President. ~~(TS//SI//NF)~~

Comey also described Ashcroft as being frustrated, and said he was "beating himself up" because he was "in a box" with Yoo, yet was learning from Philbin, Goldsmith, and now Comey that parts of the program were not in their view legally supportable.[139] ~~(TS//SI//NF)~~

After the lunch meeting on March 4, Comey traveled to Phoenix, Arizona, to make a speech. Three hours after their lunch meeting, Ashcroft was struck with severe gallstone pancreatitis and was admitted to the

---

[138] Mueller told us he maintained the program log because "[t]hese were extraordinary circumstances about which I would one day be questioned." Mueller said the program log was drafted "relatively contemporaneously" with the events described in it. (U)

[139] By the time Ashcroft received OLC's preliminary findings concerning the legality of the program in December 2003, he had already certified the program as to form and legality approximately 20 times. ~~(TS//SI//NF)~~

George Washington University Hospital. After being informed that Ashcroft was hospitalized, Comey returned to Washington the next morning on an FBI jet. (U)

2. March 5, 2004: Comey Determines Ashcroft is "Absent or Disabled" (U)

On March 5, 2004, Goldsmith advised Comey by memorandum that under the circumstances of Ashcroft's medical condition and hospitalization, a "clear basis" existed for Comey to determine that "this is a case of 'absence or disability' of the Attorney General" within the meaning of 28 U.S.C. § 508(a). This statute provides:

> In case of a vacancy in the office of Attorney General, or of his absence or disability, the Deputy Attorney General may exercise all the duties of that office, and for purposes of section 3345 of title 5 the Deputy Attorney General is the first assistant to the Attorney General. (U)

Goldsmith's memorandum further advised Comey that he could serve as Acting Attorney General until Ashcroft's absence or disability no longer existed, and that Comey could exercise "all the power and authority of the Attorney General, unless such power or authority is required by law to be exercised by the Attorney General personally." See 28 C.F.R. § 0.15(a). Goldsmith noted in the memorandum that there are "very few duties" that can be exercised only by the Attorney General. Goldsmith wrote that, except for these duties, Comey could opt to exercise the duties of the Attorney General as Deputy Attorney General rather than as Acting Attorney General, noting, "Your office has informed us that this is your intention."[140] (U)

Goldsmith's memorandum to Comey referenced an attached draft memorandum for Comey's review, which would memorialize Comey's decision to invoke 28 U.S.C. § 508(a) in writing, although Goldsmith advised that it was not necessary to do so. The "cc" line of Goldsmith's memorandum to Comey indicated that a copy of the memorandum was also

---

[140] According to an e-mail sent on March 5, 2004, at 9:15 a.m. from OLC Special Counsel Daniel Koffsky to OLC Principal Deputy Assistant Attorney General Edward Whelan and other Department officials, among the duties that can only be exercised by the Attorney General or his designee is the authority to approve FISA applications to engage in electronic surveillance of a specific type of agent of a foreign power based on requests of certain high level officials. 50 U.S.C. § 1804(e)(2)(A). This section represents an exception to FISA's general conferral of authority on the Attorney General, a term that is defined to include the Acting Attorney General and the Deputy Attorney General. See 50 U.S.C. § 1801(g). (U)

sent to White House Counsel Gonzales.[141] As discussed below, a significant dispute between White House and Department officials later arose over whether the White House in fact received notice of Comey's decision to assume the powers of the Attorney General, whether as Deputy Attorney General or otherwise. (U)

3. March 5, 2004: Goldsmith and Philbin Seek Clarification from White House on Presidential Authorizations (U)

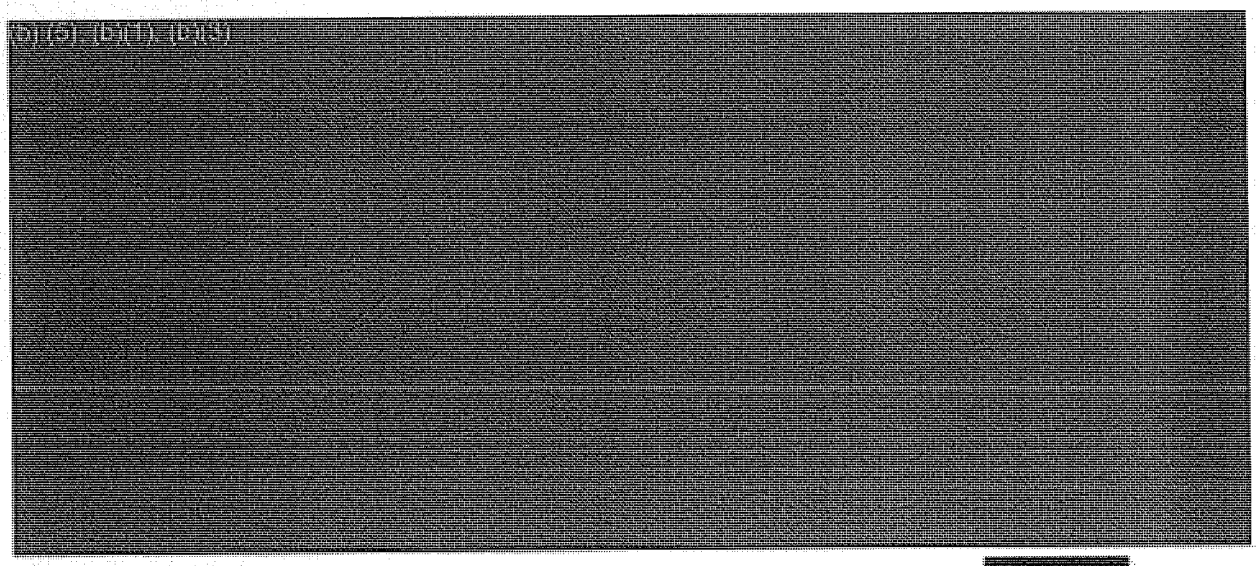
On the afternoon of Friday, March 5, 2004 – 6 days before the Presidential Authorization then in effect was set to expire – Goldsmith and Philbin met with Addington and Gonzales at the White House to seek clarification on two key issues related to the Authorizations. (U//~~FOUO~~)

First, Goldsmith expressed his belief that the [redacted] (b)(1), (b)(3), (b) (5)

Philbin said they explained to Addington and Gonzales the importance of briefing the President on this new legal approach to justifying the program. ~~(TS//STLW//SI//OC/NF)~~

Second [redacted] (b) (5) (TS//STLW//SI//OC/NF)

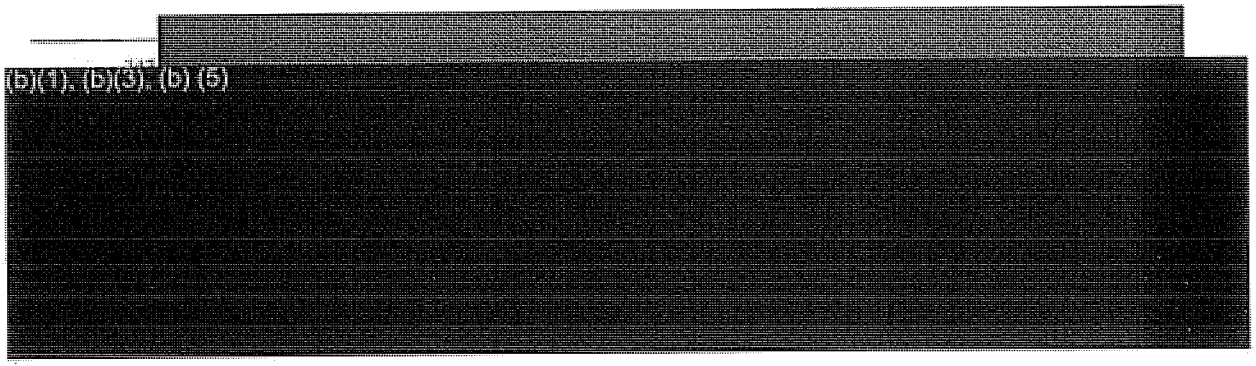
[141] A March 12, 2004, e-mail from Ashcroft's Chief of Staff David Ayres to Deputy White House Counsel David Leitch detailing the Department's efforts to inform the White House Counsel's Office of Ashcroft's hospitalization and Comey's assumption of Ashcroft's duties shows that Ayres confirmed the White House's receipt of a facsimile from OLC advising the White House of Comey's decision to exercise "all the power and authority of the Attorney General . . . in [his] capacity as Deputy Attorney General." Ayres also wrote in the e-mail that a copy of OLC's "legal memorandum" was sent to White House Counsel Gonzales. Ayres also wrote in the e-mail that he personally called Harriet Miers, a White House Deputy Chief of Staff, and informed her that Comey "had assumed the Attorney General's responsibilities[.]" Ayres wrote in the e-mail that he also informed others at the White House of Comey's status, including another White House Deputy Chief of Staff [Joe Hagin] and the White House Cabinet Secretary [Brian Montgomery]. (U)



However, according to Gonzales, Goldsmith's conclusion (b) (5), (b)(1), (b)(3) created a serious issue. Gonzales stated that Goldsmith's argument on this point was that Congress had spoken on the matter by enacting FISA, but Yoo previously had opined that FISA was unconstitutional to the extent it infringed on the President's Commander-in-Chief authority to conduct electronic surveillance without a judicial warrant.[142] (~~TS//STLW//SI//OC/NF~~)

Gonzales also told us that the March 5, 2004, meeting with Goldsmith and Philbin represented the first substantively detailed discussion he had with the OLC officials regarding their concerns with the existing legal analysis and their reservations about continuing the program as it had been operating. As noted above, Goldsmith said that he had informed Gonzales and Addington about his general concerns with Yoo's legal analysis of the program as early as December 2003. ~~(TS//SI//NF)~~

Later that day on March 5, Gonzales called Goldsmith to request a letter from the OLC stating that Yoo's prior OLC opinions "covered the program." Philbin told the OIG that Gonzales was not requesting a new



opinion that the program itself was legal, but only that the prior opinions had concluded that it was. ~~(TS//SI//NF)~~

4. March 6 to 8, 2004: The Department Concludes That Yoo's Legal Memoranda Did Not Cover the Program (U)

As a result of Gonzales's request on March 5, Goldsmith re-examined Yoo's memoranda with a view toward determining whether they adequately described the actual collection activities of the NSA under the Authorizations. Goldsmith told us that after a brief review, he called Philbin to tell him he agreed with Philbin's assessment that Yoo's memoranda were problematic from a factual standpoint. Philbin said that through this re-examination he and Goldsmith confirmed Philbin's initial sense that Yoo's memoranda did not describe the (b)(1), (b)(3) [143]

~~(TS//STLW//SI//OC/NF)~~

(b) (5), (b)(1), (b)(3)

Goldsmith's account of the response to Gonzales's request was similar. Goldsmith also stated that his and Philbin's conclusion that Yoo's memoranda failed to adequately describe the (b)(1), (b)(3) meant that OLC could not tell the White House that the program could continue under the authority of those legal memoranda. Goldsmith stated that he and Philbin realized at this point that the program had been conducted for 2 years without a proper OLC review. Specifically, both Goldsmith and Philbin stated that they had always viewed Yoo's legal analysis as poorly reasoned; however, they were now realizing that Yoo's factual description of the program was inaccurate and incomplete as well, and thus did not "cover" aspects of the program. Goldsmith said Gonzales's request for ratification of Yoo's memoranda "forced [the Office of Legal

[143]

(b) (5), (b)(3)

Counsel's] hand" and was the point at which the "presumption in favor of legality flipped."[144] ~~(TS//STLW//SI//OC/NF)~~

On Saturday, March 6, 2004, Goldsmith and Philbin advised Comey that they believed the (b) (5), (b)(1), (b)(3) Goldsmith also told Comey that the White House would have to be notified of this development. Comey agreed with this recommendation. ~~(TS//STLW//SI//OC/NF)~~

Later on March 6, Goldsmith and Philbin went to the White House to meet with Addington and Gonzales to convey their conclusions that the (b) (5), (b)(1), (b)(3) According to Goldsmith's chronology of these events, Addington and Gonzales "reacted calmly and said they would get back with us." Goldsmith told us that the White House was now worried that it was "out there," meaning that it was implementing a program without legal support. ~~(TS//STLW//SI//OC/NF)~~

On Sunday afternoon, March 7, 2004, Goldsmith and Philbin met again with Addington and Gonzales at the White House.[145] According to Goldsmith, the White House officials informed Goldsmith and Philbin that they disagreed with Goldsmith and Philbin's interpretation of Yoo's memoranda and on the need to change the scope of the NSA's collection.[146] Gonzales told us he recalled the meetings of March 6 and 7, 2004, but did not recall the specifics of the discussions. He said he remembered that the overall tenor of the meetings with Goldsmith was one of trying to "find a way forward."[147] ~~(TS//SI//NF)~~

---

[144] As noted in Chapter Three, Gonzales told us that he believed Yoo's memoranda described as lawful activities that were broader than those carried out under Stellar Wind, and that therefore these opinions "covered" the Stellar Wind program. ~~(TS//SI//NF)~~

[145] Gonzales told us that White House Chief of Staff Card may also have been present for this meeting. Goldsmith's chronology indicates that only Addington and Gonzales were present. (U)

[146] In discussing these early March meetings with the OIG, Goldsmith told us that Addington had stated on more than one occasion that Goldsmith was the head of OLC and if he determined that the program needed to be shut down, it would be shut down. Goldsmith told us he believed that the White House officials' references to "shutting down the program" extended only to those aspects of the program for which no legal support could be found. Goldsmith also told us that he did not know whether Addington and Gonzales were keeping the President informed of OLC's concerns. ~~(TS//SI//NF)~~

[147] As noted above, Gonzales was represented by counsel during his interview with the OIG. Also present during the interview because of the issue of executive privilege was a Special Counsel to the President, Emmitt Flood. We asked Gonzales whether the President had been informed by this point in time of the OLC position regarding the lack of legal (Cont'd.)

On the evening of Sunday, March 7, 2004, Goldsmith and Philbin met with Comey in Comey's office to again review Yoo's opinions and make sure all three agreed with the conclusion that the opinions failed to support the Stellar Wind program as it was being implemented. Philbin said that until Gonzales's March 5 request for a letter from the OLC stating that Yoo's prior OLC opinions "covered the program," he and Goldsmith had intended to recommend that the program be recertified on March 11, 2004, while they continued to work on the new OLC opinion. (b) (5), (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~

According to Goldsmith's chronology, there was no interaction with the White House on the issue on the following day, Monday, March 8, 2004. Goldsmith wrote in his chronology of events for this day: "Monday, March 8: Silence." (U)

5. March 9, 2004: White House Seeks to Persuade Department and FBI to Support Continuation of the Program ~~(S//NF)~~

On Tuesday, March 9, 2004, Gonzales called Goldsmith to attend an early morning meeting (at 6:00 or 6:30 a.m.) at the White House to discuss the issues regarding Yoo's memoranda and the Stellar Wind program.[149] Goldsmith called Philbin and told him to meet Goldsmith at the White House. According to Goldsmith, Philbin was allowed into the White House, but Gonzales excluded Philbin from the meeting despite Goldsmith's requests that Philbin be allowed to participate. ~~(S//NF)~~

---

support for the program and (b) (5), (b)(1), (b)(3). Flood objected to the question on relevancy grounds and advised Gonzales not to answer, and Gonzales did not provide us an answer. However, when Gonzales commented on a draft of this report, he stated that he would not have brought Goldsmith and Philbin's "concerns" to the attention of the President because there would have been nothing for the President to act upon at that point. Gonzales stated that this was especially true given that Ashcroft continued to certify the program as to legality during this period. Gonzales stated he generally would only bring matters to the President's attention if the President could make a decision about them. ~~(TS//STLW//SI//OC/NF)~~

148 (b) (5), (b)(1), (b)(3)

149 Gonzales told the OIG that he did not recall this meeting. Both Goldsmith and Philbin told the OIG about the meeting. The meeting is also briefly described in Goldsmith's contemporaneous notes and chronology. (U)

Goldsmith said Gonzales tried first to persuade him that he and Philbin were wrong to conclude that Yoo's memoranda did not provide sufficient legal justification to cover the parts of the program that OLC had identified as problematic, but that Gonzales did not persuade him on this point. Gonzales next argued for a "30-day bridge" to get past the upcoming March 11, 2004, Authorization. Gonzales reasoned that Ashcroft, who was still hospitalized, was not in any condition to sign the upcoming Authorization, and that a "30-day bridge" would move the situation to a point where Ashcroft would be well enough to approve the program. Goldsmith told Gonzales he could not agree to recommend an extension. ~~(TS//SI//NF)~~

Goldsmith said Gonzales noted that Ashcroft had certified the program as to form and legality for the previous two and a half years, yet now Comey was the Acting Attorney General. Goldsmith said the implication of Gonzales's statement was that not approving the March 11, 2004, Authorization would "undercut" Ashcroft. Goldsmith said he made clear to Gonzales that Ashcroft was "supportive" of his and Philbin's analysis. Goldsmith's notes from the meeting also indicate that Gonzales stated that he did not "want to face" Ashcroft in the hospital. Goldsmith told us he recommended to Gonzales that he not visit Ashcroft.[150] ~~(TS//SI//NF)~~

Goldsmith said his discussion with Gonzales lasted about 1 hour. Philbin was then brought into Gonzales's office and the issues were discussed again. According to Goldsmith's chronology, nothing was resolved during the meeting. (U)

At noon that day, another meeting was held in Andrew Card's office at the White House. According to Director Mueller's program log, Mueller, Chief of Staff Card, Vice President Cheney, CIA Deputy Director John McLaughlin, Hayden, Gonzales, and other unspecified officials were present. Comey, Goldsmith, and Philbin were not invited to this meeting. Mueller described this gathering as a "pre-meeting" in anticipation of another meeting that was to be held later that afternoon in which the Justice Department officials (Comey, Goldsmith, and Philbin) would be participating.[151] (U)

---

[150] At noon on March 9, 2004, Attorney General Ashcroft underwent surgery at the George Washington University Hospital. The surgery was completed by 2:30 p.m. (U)

[151] Mueller prepared for this meeting by meeting earlier that morning with Michael Fedarcyk, the Chief of the FBI's Communications Exploitation Section; General Counsel Valerie Caproni; and possibly others. Mueller's program log indicates that Fedarcyk "appears unaware of details of how [redacted] is collected." ~~(TS//SI//NF)~~

According to Mueller's notes, a presentation on the value of the Stellar Wind program was given by CIA and NSA representatives.[152] It was then explained to the group that Comey "has problems" with (b)(1), (b)(3) Mueller's notes state that Vice President Cheney suggested that "the President may have to reauthorize without [the] blessing of DOJ," to which Mueller responded, "I could have a problem with that," and that the FBI would "have to review legality of continued participation in the program." ~~(TS//STLW//SI//OC/NF)~~

A third meeting was held at the White House that afternoon, at 4:00 p.m. The meeting included Comey, Goldsmith, and Philbin, in addition to Vice President Cheney, Card, Addington, Gonzales, Hayden, Mueller, CIA General Counsel Muller, McLaughlin, and approximately 10 NSA analysts. Gonzales told us the meeting was held to make sure that Comey understood what was at stake with the program and to demonstrate its value. ~~(S//NF)~~

At the beginning of the meeting the NSA analysts made a presentation to Comey, Goldsmith, and Philbin. Comey said the presentation consisted of charts showing the chaining (b)(1), (b)(3) capabilities that could be generated from Stellar Wind-derived information, as well as a description of "success stories" resulting from the program. Comey told us that the cases the analysts highlighted were not in his view the Stellar Wind successes that the analysts claimed, and that he felt "the NSA had no good stories to tell about the program."[153] Comey also told us that the collection of content communications under Stellar Wind was somewhat duplicative of existing FISA coverage, and that only the meta data collection under baskets 2 and 3 represented truly new capabilities. However, Comey said he did not challenge the analysts on the assertion that Stellar Wind was a critical anti-terrorism tool because the value of the program was not his primary concern. Rather, Comey said he was willing to concede the program's value, and that his concern was with its legality. ~~(TS//STLW//SI//OC/NF)~~

Goldsmith told us that he did not believe it was his place to judge the value of the program from an intelligence-gathering standpoint. Goldsmith told us he found persuasive a remark by Hayden that even though there may not have been major successes under the program to date, the program still could produce successes in the future. However, both Goldsmith and

---

[152] Mueller's notes indicate that [redacted] were cited as examples during the presentation. We discuss [redacted] briefly in this chapter and [redacted] in Chapter Six. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7E, b7C

[153] Comey specifically questioned whether the [redacted] case was a legitimate "success story" under the Stellar Wind program. The [redacted] case, as well as other cases cited as successes under Stellar Wind, is discussed in Chapter Six. b1, b3, b6, b7E, b7C
~~(TS//STLW//SI//OC/NF)~~

Philbin told us that they believed that identifiable successes under the program [redacted]
(b)(1), (b)(3), (b) (5)
[redacted]
~~(TS//STLW//SI//OC/NF)~~

The NSA analysts were excused after their presentation and the meeting continued. Comey said Vice President Cheney stressed that the program was "critically important" and warned that Comey would risk "thousands" of lives if Comey did not agree to recertify it. Comey said he told those at the meeting that he, as the Deputy Attorney General exercising the powers of the Attorney General, could support reauthorizing [redacted] (b)(1), (b)(3) [154] However, he told the group "we can't get there" on (b)(1), (b)(3) [redacted] According to Comey, the White House said it could not agree to that modification. ~~(TS//STLW//SI//OC/NF)~~

Comey also told us he was certain the White House understood him to be the acting in Attorney General Ashcroft's stead during this meeting. (U)

(b)(1), (b)(3), (b)(5) [redacted]

Gonzales told us that he came away from the meeting with the understanding that Comey (b)(1), (b)(3) [redacted] ~~(TS//STLW//SI//OC/NF)~~

6. Conflict Ensues between Department and White House (U)

Each of the Department witnesses we interviewed concerning the Department's discussions with the White House during this time period

[154] (b)(1), (b)(3), (b)(5) [redacted]

emphasized the sense of pressure and anxiety that pervaded the discussions in March 2004. For instance, Comey said discussions during the meeting at the White House on March 9 became heated as he sought to convey to everyone how difficult it was for the Department to take the position it was taking, and how hard the Department officials were working to find a solution. Comey also stated that Vice President Cheney was "understandably frustrated" because the Department was changing its advice to the White House about the program. (U)

Goldsmith also recalled that at one point during these meetings with the White House, Addington told him that if he narrowed the Stellar Wind program Goldsmith "will have the blood of 100,000 American lives on his hands." ~~(S//NF)~~

Goldsmith observed to us that from the White House's point of view, due to the timing of the events, and in particular with Ashcroft in the hospital, it appeared to the White House that a "palace coup" was taking place at the Department of Justice. Goldsmith said that this perception was somewhat understandable under the circumstances. (U)

Philbin also stated that tensions were high during this period and that the Department and White House "started to divide into camps." Philbin added that Department and White House officials were "starting to attribute motives" to each other. Philbin said he thought Addington came to believe that Comey was opposed to recertifying the program for "political reasons," and that Comey wanted to be on the "politically right" side of the dispute. (U)

Comey said that his dealings with Gonzales, Card, Addington, and others at the White House were generally civil. Comey acknowledged that there was tension between the Department and the White House during the March 2004 period, but believed that it resulted primarily from differences in legal perspectives. (U)

II. White House Continues Program without Justice Department's Certification ~~(TS//SI//NF)~~

The Presidential Authorization under which the program was operating during early 2004 was set to expire on March 11, 2004. As described in the preceding section, Comey concurred with the views of Goldsmith and Philbin, and as the Deputy Attorney General exercising the powers of the Attorney General Comey refused to certify the program as to form and legality. He conveyed this decision to the White House during the meeting on the afternoon of March 9, 2004. In response, as described below, the President decided to reauthorize the program without the Justice

Department's support, precipitating a serious confrontation between White House and Department officials. ~~(TS//STLW//SI//OC/NF)~~

A. White House Counsel Gonzales Certifies March 11, 2004, Presidential Authorization ~~(TS//SI//NF)~~

1. March 10, 2004: Office of Legal Counsel Presses for Solicitor General to be Read into Program (U)

Goldsmith, Philbin, and Comey met in the early afternoon of March 10, 2004, to discuss the meeting at the White House the day before and how the Department should proceed. Goldsmith and Philbin reconfirmed their position to Comey that collection under (b) (5), (b)(1), (b)(3) [redacted] ~~(TS//STLW//SI//OC/NF)~~

Goldsmith and Philbin also recommended to Comey that Solicitor General Theodore Olson be read into the program. Goldsmith told us that Olson had been at the Department for a long time and had valuable experience and credibility. Goldsmith said that given the importance of the decisions being made at the Department concerning the program at this time, he believed it was imperative to have Olson read in. (U)

Comey agreed with Goldsmith and Philbin, and he directed Goldsmith to call Gonzales to reaffirm the Department's position on the program and also to request that Olson be read in. (U)

Goldsmith called Gonzales at 2:20 p.m. on March 10 to tell him that the Department could not support the legality of (b)(1), (b)(3), (b) (5) [redacted] as then being implemented under the program. Goldsmith also told Gonzales of the "urgent need" for approval to read Olson into the program. Goldsmith's notes indicate that he called Gonzales twice that day with the request to have Olson read in, but by early evening had not heard back from Gonzales. ~~(TS//STLW//SI//OC/NF)~~

2. March 10, 2004: Congressional Leaders Briefed on Situation (U)

Gonzales told us that after President Bush was advised of the results of the March 9, 2004, meeting, the President instructed Vice President Cheney on the morning of Wednesday, March 10, to call a meeting with congressional leaders to advise them of the impasse with the Justice Department. On the afternoon of March 10, at approximately 4:00 or 5:00 p.m., Gonzales and other White House and intelligence agency officials, including Vice President Cheney, Card, Hayden, McLaughlin, and Director of Central Intelligence George Tenet, convened an "emergency meeting" with Congressional leaders in the White House Situation Room. The

congressional leaders in attendance were Senate Majority and Minority Leaders Bill Frist and Tom Daschle; Senate Select Committee on Intelligence Chairman Pat Roberts and Vice Chairman Jay Rockefeller; Speaker of the House Dennis Hastert and House Minority Leader Nancy Pelosi; and House Permanent Select Committee on Intelligence Chair Porter Goss and Ranking Member Jane Harman. This congressional group was known informally as the "Gang of Eight." (U)

No officials from the Department were present at the meeting. When we asked Gonzales whether the White House had given any consideration to inviting Department officials to attend, Gonzales declined to answer on the advice of the Special Counsel to the President, who was present during Gonzales's interview with the OIG.[155] (U)

Gonzales told us that President Bush also directed him to "memorialize" the meeting, although Gonzales said he could not recall whether the President directed him to do so before or after the meeting. Gonzales did not take notes during the meeting. Rather, he said he wrote down his recollection of the meeting within a few days of Wednesday, March 10, probably, according to him, the following weekend.[156] Gonzales said that, with the exception of a single phrase discussed below, he wrote his notes in one sitting in his White House office. (U)

The notes indicate that President Bush appeared briefly at the start of the meeting to explain how important the meeting was. Vice President Cheney, who chaired the meeting, gave a general explanation of the program and indicated that the purpose of the meeting was to "discuss potential legislation to continue the program." According to Gonzales's notes, Hayden then explained the collection of "telephone content and meda data [sic]" under the program. (b)(1), (b)(3)

---

[155] However, when Gonzales commented on a draft of this report, he stated that the Department was not invited to the meeting because the purpose of the meeting was to advise the congressional leaders that a legislative fix was necessary, not to describe or resolve the legal dispute between the Department and the White House. (U//~~FOUO~~)

[156] Gonzales's handling of his notes from this meeting later became the subject of a separate OIG misconduct investigation. The OIG found that when Gonzales became the Attorney General in 2005, he took the notes, which contained TS/SCI information relating to the Stellar Wind program, from the White House and improperly stored these notes at his residence for an indeterminate period. When he brought the notes to the Justice Department, he kept them in a safe near his office that was not cleared for storage of TS/SCI material. The OIG also determined through this investigation that Gonzales improperly stored several other TS/SCI documents in the safe near his office, many of which concerned Stellar Wind. The OIG's report, entitled "Report of Investigation Regarding Allegations of Mishandling of Classified Documents by Attorney General Alberto Gonzales," was released by the OIG on September 2, 2008, and can be found at http://www.usdoj.gov/oig/special/s0809/index.htm. ~~(S//NF)~~

(b)(1), (b)(3) '[157] According to Gonzales's notes, the briefers then left the meeting and the remaining participants discussed the need for legislation so that the program's intelligence collection activities could continue. ~~(TS//STLW//SI//OC/NF)~~

Gonzales's notes indicate that when he was asked at the meeting why Comey was "reluctant" to sign the Authorization, Gonzales responded, "I said it was not really my place to represent [Comey's] position, but I believed that he did not feel that the President's Constitutional authority would not [sic] override FISA." The notes do not indicate what else was discussed about the basis for the Department's concerns about the legal support for the program. ~~(TS//STLW//SI//OC/NF)~~

The notes indicate that Andrew Card stated that "it would be hard to explain if another attack occurred and we could have stopped it with this tool." Gonzales's notes then state:

- Andy asked if anyone had any reservation and no one spoke up raising an objection
- The VP said that what I am hearing is that we should go forward with the program for a period of 30-45 days and see if there was a legislative fix. ~~(TS//SI//NF)~~

The notes indicate that Vice President Cheney read aloud proposed language of new legislation. However, the notes do not describe the proposed legislation that was discussed. (U)

According to Gonzales's notes, the reactions and comments of the congressional leaders were as follows: Both Hastert and Roberts "said they now felt an obligation to use the tool," although according to the notes Hastert "kept coming back to the (b)(1), (b)(3) Roberts said that if Comey would not certify the Authorization "he should be fired." Harman suggested that another branch of government "should have some role, checks and balances on the program" and raised the possibility of involving the FISA Court. According to the notes, Gonzales responded to Harman's suggestion by volunteering that it would be possible to have the Presiding Judge of the FISA Court "approve or develop the guidelines to protect privacy rights." The notes state that Daschle felt it would be "impossible to get [new legislation] passed

[157] Gonzales told us he was unable to recall (b)(1), (b)(3) he was referring to in the notes, and said he did not recall whether it had to do with (b)(1), (b)(3) (U)

without it becoming very public." Rockefeller was "concerned about privacy safeguards" and was advised of "the 39 steps followed [by the NSA] to make sure privacy concerns were addressed." According to the notes, Pelosi expressed concern about giving "total discretion" to the President and discussed the need for the proposed legislation to be periodically renewed by Congress and that it not be permanent. ~~(TS//STLW//SI//OC/NF)~~

Gonzales told us he initially left a gap in one section of the notes where he described Pelosi's comments. He stated that a day or so later, after recalling what she had said at the meeting, he filled in the gap with the following italicized language: "Pelosi said *tell DAG that everyone is comfortable* and the program should go forward."[158] (U)

3. March 10, 2004: Hospital Visit (U)

Gonzales told us that following the meeting with the congressional leaders during the afternoon of March 10, President Bush instructed him and Card to go to the George Washington University Hospital to speak to Ashcroft, who was recovering from surgery in the intensive care unit. The events that followed, which are recounted below, are based on notes from Ashcroft's FBI security detail, Goldsmith's notes, and Mueller's program log; the OIG's interviews of Gonzales, Comey, Goldsmith, Philbin, and Mueller; and Comey and Gonzales's congressional testimony.[159] (U)

At 6:20 p.m. on March 10, Card called the hospital and spoke with an agent in Ashcroft's FBI security detail, advising the agent that President Bush would be calling shortly to speak with Ashcroft. Ashcroft's wife told

---

[158] When Gonzales testified before the Senate Judiciary Committee on July 24, 2007, he essentially described the congressional leaders' reactions to the March 10, 2004, Gang of Eight briefing as he did in his handwritten notes of the briefing, stating, "The consensus in the room from the congressional leadership is that we should continue the activities, at least for now." However, after Gonzales testified, Representative Pelosi, Senator Rockefeller, and Senator Daschle issued statements to the media sharply disputing Gonzales's characterization of their statements at the March 10, 2004, briefing, and stating that there was no consensus at the meeting that the program should proceed. See "Gonzales, Senators Spar on Credibility," by Dan Eggen and Paul Kane, The Washington Post (July 25, 2007). Pelosi's office also issued a statement that she "made clear my disagreement with what the White House was asking" concerning the program. See "Gonzales Comes Under New Bipartisan Attack in Senate," by James Rowley, Bloomberg.com (July 24, 2007). We did not attempt to interview the congressional leaders and obtain their recollections as to what was said at this meeting, because this was beyond the scope of our review. (U)

[159] Comey described the events surrounding the hospital visit in testimony before the Senate Judiciary Committee on May 15, 2007. Gonzales testified about these issues before the Senate Judiciary Committee on July 24, 2007. As noted above, Attorney General Ashcroft and Card declined our request to be interviewed. Ayres, Ashcroft's Chief of Staff at the time, also declined our request for an interview. (U)

the agent that Ashcroft would not accept the call. Ten minutes later, the agent called Ashcroft's Chief of Staff David Ayres through the Justice Command Center to request that Ayres speak with Card about the President's intention to call Ashcroft. The agent conveyed to Ayres Mrs. Ashcroft's desire that no calls be made to Ashcroft for another day or two.[160] Ayres told the agent he would relay this message to Card. (U)

However, at 6:45 p.m., Card and the President called the hospital and, according to the agent's notes, "insisted on speaking [with Attorney General Ashcroft]." According to the agent's notes, Mrs. Ashcroft, rather than Attorney General Ashcroft, took the call from Card and the President. According to the agent's notes, she was informed that Gonzales and Card were coming to the hospital to see Ashcroft regarding a matter involving national security. (U)

At approximately 7:00 p.m., Ayres was advised, either by Mrs. Ashcroft or a member of the Attorney General's security detail that Gonzales and Card were on their way to the hospital. Ayres then called Comey, who at the time was being driven home by his security detail, and told Comey that Gonzales and Card were on their way to the hospital. Comey told his driver to rush him to the hospital. According to Comey, his driver activated the emergency lights on the vehicle and headed to the hospital. (U)

According to his congressional testimony, Comey then called his Chief of Staff, Chuck Rosenberg, and directed him to "get as many of my people as possible to the hospital immediately." Comey then called FBI Director Mueller, who was having dinner with his wife and daughter at a restaurant, and told him that Gonzales and Card were on their way to the hospital to see Ashcroft, and that Ashcroft was in no condition to receive guests, much less make a decision about whether to continue the program. According to Mueller's program log, Comey asked Mueller to come to the hospital to "witness [the] condition of AG." Mueller told Comey he would go to the hospital right away. (U)

At 7:05 p.m., Ayres was notified by an agent on Ashcroft's security detail that Comey was en route to the hospital. Ayres called the agent back at approximately 7:20 p.m. and told the agent that "things may get 'a little weird'" when Gonzales and Card arrived. Ayres instructed Ashcroft's security detail, which was composed of FBI agents, to give its "full support" to Comey and to follow Comey's instructions. Ayres also told the agent that the security detail should not allow the U.S. Secret Service agents who

---

[160] Ashcroft was recovering from his gallbladder surgery the prior day. He was described by those who saw him that night as being very weak and appearing heavily medicated. Philbin told us that Ashcroft was "on morphine" on the evening of March 10. (U)

would be accompanying Gonzales and Card to remove Comey from Ashcroft's room. The FBI agent told Ayres that the Attorney General's security detail would "fully back" Comey and that "this is 'our scene'." (U)

Philbin said he was leaving work that evening when he received a call from Comey, who said that Philbin needed to get to the hospital right away because Gonzales and Card were on their way there "to get Ashcroft to sign something." Comey also directed Philbin to call Goldsmith and tell him what was happening at the hospital. Philbin called Goldsmith from a taxi on his way to the hospital. Goldsmith told us he was home having dinner when he received Philbin's call telling him to go immediately to the hospital. (U)

Comey arrived at the hospital between 7:10 and 7:30 p.m.[161] In his congressional testimony, Comey said he ran up the stairs with his security detail to Ashcroft's floor, and he entered Ashcroft's room, which he described as darkened, with Ashcroft lying in bed and his wife standing by the bed. Comey said he began speaking to Ashcroft, "trying to orient him as to time and place, and try to see if he could focus on what was happening." Comey said it was not clear that Ashcroft could focus and that he "seemed pretty bad off[.]" Comey stepped out of the room into the hallway and telephoned Mueller, who was on his way to the hospital. With Mueller still on the line, Comey gave his phone to an FBI agent on Ashcroft's security detail, and according to Comey Mueller instructed the agent not to allow Comey to be removed from Ashcroft's room "under any circumstances." (U)

Goldsmith and Philbin arrived at the hospital within a few minutes of each other. Comey, Goldsmith, and Philbin met briefly in an FBI "command post" that had been set up in a room adjacent to Ashcroft's room. Moments later, word was received at the command post that Card and Gonzales had arrived at the hospital and were on their way upstairs to see Ashcroft. Philbin told us the FBI agents in the command post called down to the checkpoint at the hospital entrance to ask whether Card and Gonzales were accompanied by Secret Service agents, which Philbin said indicated concern that a "stand-off" between the FBI agents and the Secret Service agents might ensue. (U)

Comey, Goldsmith, and Philbin entered Ashcroft's room. Goldsmith described Ashcroft's appearance as "weak" and "frail," and observed that his breathing was shallow. Philbin said he was shocked by Ashcroft's appearance and said he "looked terrible." Philbin said that Ashcroft

---

[161] There is a discrepancy in the Attorney General's security detail log on the time. One agent wrote that Comey arrived at 7:10. Another agent wrote that Comey arrived at 7:30. (U)

appeared to have lost a lot of weight, was "gray in the face," and was "almost out of it" because he was on morphine. Comey stated that Ashcroft was "clearly medicated." (U)

Comey testified that he sat in an armchair by the head of Ashcroft's bed, with Goldsmith and Philbin standing behind him; Mrs. Ashcroft stood on the other side of the bed holding Ashcroft's arm. No security or medical personnel were present. (U)

Goldsmith's notes indicate that at this point Comey and the others advised Ashcroft "not to sign anything." (U)

Gonzales and Card, unaccompanied by Secret Service agents, entered Ashcroft's hospital room at 7:35 p.m., according to the FBI agent's notes.[162] The two stood across from Mrs. Ashcroft at the head of the bed, with Comey, Goldsmith, and Philbin behind them. (U)

Gonzales stated that when he entered the hospital room, Ashcroft was in the bed and his wife was "at the 11:00 position." Gonzales said to us that he was unaware that Comey, Goldsmith, and Philbin were also present in the room until Card told him this later. Gonzales told us that he could "sense" that others were in the room, but that he was not sure who, because his focus was on Ashcroft. Gonzales said he carried with him in a manila envelope the March 11, 2004, Presidential Authorization for Ashcroft to sign. (U)

According to Philbin, Gonzales first asked Ashcroft how he was feeling. Ashcroft replied, "Not well." Gonzales then said words to the effect, "You know, there's a reauthorization that has to be renewed . . . ." (U)

Goldsmith told the OIG that Gonzales next reminded Ashcroft that he had been certifying the program for the past 2 years. Comey told us that Gonzales told Ashcroft, "We have arranged for a legislative remediation; we're going to get Congress to fix it," and that more time was needed to accomplish this. Comey told us he did not know what Gonzales meant by "legislative remediation." (U)

Gonzales told us that he did not recall telling Ashcroft that a legislative remediation had been arranged, but rather may have told Ashcroft that White House officials had met with congressional leaders "to pursue a legislative fix." (U)

Comey testified to the Senate Judiciary Committee about what happened next:

---

[162] Gonzales told us he and Card arrived in Ashcroft's hospital room at 7:20. (U)

> . . . Attorney General Ashcroft then stunned me. He lifted his head off the pillow and in very strong terms expressed his view of the matter, rich in both substance and fact, which stunned me, drawn from the hourlong meeting we'd had a week earlier, and in very strong terms expressed himself, and then laid his head back down on the pillow. He seemed spent. . . . And as he laid back down, he said, "But that doesn't matter, because I'm not the Attorney General. There is the Attorney General," and he pointed to me – I was just to his left. The two men [Gonzales and Card] did not acknowledge me; they turned and walked from the room. (U)

Comey also testified that "I thought I had just witnessed an effort to take advantage of a very sick man, who did not have the powers of the Attorney General because they had been transferred to me." (U)

Philbin described to us Ashcroft's statements to Gonzales and Card in the hospital room, stating that Ashcroft "rallied and held forth for two minutes" about problems with the program as had been explained to him by Comey, and that Ashcroft agreed with Comey. Gonzales told us that he did not recall Ashcroft stating that he agreed with Comey. Goldsmith's notes indicate that Ashcroft argued in particular that NSA's collection activities exceeded the scope of the Authorizations and the OLC memoranda, stating that he was troubled by [redacted]"[163] According to Goldsmith's notes Ashcroft also said that it was "very troubling that [redacted] people in other agencies" had been read into the program, but that Ashcroft's own Chief of Staff, and until recently the Deputy Attorney General, had not been allowed to be read in. Gonzales told us he responded to Ashcroft that this was the President's decision. ~~(TS//SI//NF)~~

According to Goldsmith's notes, Ashcroft also complained that the White House had "not returned phone calls," and that the Department had been "treated badly and cut out of [the] whole affair." Ashcroft told Gonzales that he was "not prepared to sign anything." (U)

When we interviewed Gonzales about the hospital visit, he stated that these were "extraordinary circumstances," that the program had been reauthorized over the past two years, and that the sentiment of the

---

[163] As discussed in Chapter Three, Ashcroft was present for the January 31, 2002, briefing of Presiding Judge of the FISA Court Royce Lamberth about the program. According to an outline of information to be covered during that briefing, NSA Director Hayden would have explained how the program functioned operationally. Because Ashcroft did not agree to be interviewed, we were unable to determine what Ashcroft understood about the [redacted] collection prior to Philbin and Goldsmith's explanation to him of this aspect of the program in late 2003. ~~(TS//STLW//SI//OC/NF)~~

congressional leadership was that it should continue. Gonzales said he therefore felt it was very important that Ashcroft be told what was happening, adding "If I were the Attorney General I would damn sure want to know." (U)

In his July 2007 congressional testimony, Gonzales also explained the visit to the hospital by stating that it was "important that the Attorney General knew about the views and recommendations of the congressional leadership; that as a former member of Congress and as someone who had authorized these activities for over two years, that it might be important for him to hear this information. That was the reason that Mr. Card and I went to the hospital." Gonzales further testified, "We didn't know whether or not he knew of Mr. Comey's position and, if he did know, whether or not he agreed with it." Gonzales also disputed Goldsmith's account that Ashcroft stated that he was "not prepared to sign anything," and referred us to his July 2007 testimony where he stated: (U)

> My recollection, Senator [Feinstein], is – and, of course, this happened some time ago and people's recollections are going to differ. My recollection is that Mr. Ashcroft did most of the talking. At the end, my recollection is, he said, "I've been told it would be improvident for me to sign. But that doesn't matter, because I'm no longer the Attorney General." (U)

Gonzales told us that he and Card would not have gone to the hospital if they believed Ashcroft did not have the authority to certify the Authorization and told us that as soon as Ashcroft stated he no longer retained authority to act, Gonzales decided not ask Ashcroft to sign the Authorization. In his congressional testimony Gonzales stated, "Obviously there was concern about General Ashcroft's condition . . . [W]e knew, of course, that he was ill, that he'd had surgery." Gonzales also stated that "We would not have sought nor did we intend to get any approval from General Ashcroft if in fact he wasn't fully competent to make that decision." He also testified, "There's no governing legal principle that says that Mr. Ashcroft [. . .] If he decided he felt better, could decide, 'I'm feeling better and I can make this decision, and I'm going to make this decision.'"[164] (U)

The Attorney General security detail's logs indicate that Gonzales and Card left Ashcroft's room at 7:40 p.m. (U)

---

[164] Hearing before Senate Judiciary Committee, July 24, 2007. Gonzales also told us that he would not have gone to the hospital solely over the dispute concerning the scope [redacted] ~~(TS//SI//NF)~~

Moments after Gonzales and Card departed, Mueller arrived at the hospital. According to Mueller's notes, outside the hospital room Comey informed him of the exchange that had occurred in Ashcroft's room, and in particular that Ashcroft had stated that Comey was the Acting Attorney General, that "all matters" were to be taken to Comey, but that Ashcroft supported Comey's position regarding the program. Mueller's notes also state: "The AG also told [Gonzales and Card] that he was barred from obtaining the advice he needed on the program by the strict compartmentalization rules of the [White House]." (U)

Mueller's notes indicate that Comey asked Mueller to witness Ashcroft's condition, and requested Mueller to inform the FBI security detail that no visitors, other than family, be allowed to see Ashcroft without Mueller's consent. Both Mueller's notes and the security detail log indicate that Mueller instructed the detail that under no circumstances was anyone to be allowed into Ashcroft's room without express approval from either Mrs. Ashcroft or Mueller. (U)

At approximately 8:00 p.m. Mueller went into Ashcroft's room for 5 to 10 minutes. Mueller wrote in his program log: "AG in chair; is feeble, barely articulate, clearly stressed." (U)

4. March 10, 2004: Olson is Read into the Program (U)

According to Comey's congressional testimony, while he was speaking with Mueller prior to Mueller's departure from the hospital, an FBI agent interrupted, stating that Comey had an urgent telephone call from Card. Comey testified that he then spoke with Card, who was very upset and demanded that Comey come to the White House immediately. Comey testified that he told Card that based on the conduct Comey had just witnessed at the hospital, he would not meet with Card without a witness present. Comey testified that Card replied, "What conduct? We were just there to wish him well." Comey reiterated his condition that he would only meet Card with a witness present, and that he intended the witness to be Solicitor General Olson. Comey testified that until he could "connect" with Olson, he was not going to meet with Card. Card asked if Comey was refusing to come to the White House, and Comey responded that he was not refusing and would be there, but that he had to go back to the Justice Department first. (U)

Comey and the other Department officials left the hospital at 8:10 p.m. Philbin stated that he returned to the Department with Comey in Comey's vehicle, and that the emergency lights were again activated. Goldsmith also left the hospital and went to the Department. At the Department Comey, Goldsmith, and Philbin were joined by Olson, who had come to the Justice Department after being contacted at a dinner party.

Comey told us that he believed there was an urgent need to have Olson read into the program because he was confident Olson would agree with Comey and the others that Yoo's legal analysis was flawed and that Olson would be a strong ally in the matter because of Olson's respected intellect and credibility. (U)

During this meeting at the Justice Department, a call came from Vice President Cheney for Olson, which Olson took on a secure line in Comey's office while Comey waited outside. Comey told us he believes Vice President Cheney effectively read Olson into the program during that conversation. (U)

Comey and Olson then went to the White House at about 11:00 p.m., and met with Gonzales and Card that evening. Comey testified that Card would not allow Olson to enter his office. Comey relented and spoke to Card alone for about 15 minutes. At that point, Gonzales arrived and brought Olson into the room. According to Comey, he communicated the Department's views on the dispute and that the dispute was not resolved in this discussion. Comey stated that Card was concerned that he had heard reports that there was to be a large number of resignations at the Department. (U)

Gonzales told us that he recalled that Comey met first with him and Card while Olson waited outside the office, and that Olson joined them shortly thereafter. Gonzales said that little more was achieved than a general acknowledgement that a "situation" continued to exist because of the disagreement between the Department and the White House regarding the program.[165] (U)

5. March 11, 2004: Goldsmith Proposes Compromise Solution (U)

According to a memorandum to the file drafted by Goldsmith, he met with Gonzales at 6:30 a.m. the next morning, March 11, 2004, at the White House to discuss a proposal under which the Department could support

---

[165] Comey stated that Olson did not become deeply involved in analyzing the Stellar Wind program in the days that followed because he was preparing for a major argument before the Supreme Court. Comey told us that Deputy Solicitor General Paul Clement was read into the program on March 12, 2004, and reviewed all of the OLC memoranda that weekend. Comey said Clement agreed with Goldsmith and Philbin's analysis "one hundred percent" and later worked with the OLC on drafting a new memorandum on the legality of the program, which is discussed below. However, Bradbury told us that Comey's characterization of Clement's view of the analysis was exaggerated. Bradbury told us that Clement had remarked to him after these events transpired that Goldsmith and Philbin's analysis "sounded reasonable to me at the time," and that Clement's view of the analysis was based only on a limited review of it. ~~(TS//SI//NF)~~

certification of the program. Goldsmith's proposal had three conditions.

[redacted] (TS//STLW//SI//OC/NF)

Goldsmith told us that he did not specifically recall this meeting. Gonzales told us that he recalled conveying to Goldsmith and Philbin at some point during this day that the President had decided he had the constitutional authority to continue the program. Gonzales said he also expressed to Department officials the sentiment that the Department should continue seeking a way to "get comfortable" with the President's decision. (U)

6. March 11, 2004: White House Asserts that Comey's Status as Acting Attorney General was Unclear (U)

Goldsmith told the OIG that later during the morning of March 11, 2004, he received a call from Deputy White House Counsel David Leitch. Goldsmith said Leitch was "yelling and screaming" about the White House not being informed that Comey was the Acting Attorney General. Goldsmith told the OIG that Leitch made two specific complaints. First, Leitch claimed that the White House had never received a determination from OLC on Comey's assumption of Ashcroft's powers and duties. Goldsmith told us that to rebut this charge, OLC Deputy Assistant Attorney General Edward Whelan was sent to the Justice Command Center to retrieve from a waste basket the facsimile transmittal confirmation sheet from the March 5, 2004, memorandum Goldsmith had sent to Gonzales entitled "Determination that Attorney General is absent or disabled." This confirmation sheet subsequently was sent to Leitch.[166] (U)

[166] In a March 12, 2004, e-mail to Ayres, Comey, Goldsmith, Philbin, and others (including a copy to Gonzales), Leitch offered a "clarification," asserting that the White House had in fact received the Goldsmith memoranda of March 5, as well as the

(Cont'd.)

Leitch's second claim was that the OLC memorandum was ambiguous because it did not specify whether the Attorney General was determined to be "absent" or "disabled," a difference for purposes of the Attorney General's authority. According to Goldsmith, if the Attorney General was "absent," the Deputy Attorney General could act as the Attorney General, although the Attorney General would retain his authority and technically could overrule the Deputy. If the Attorney General was "disabled," the Attorney General was divested of all authority. Goldsmith said he responded to Leitch by noting the inconsistency of the White House making this second claim because, according to Leitch, it had not received Goldsmith's memorandum in the first instance. (U)

Goldsmith said he also told Leitch to "lay off" the complaints, but that Leitch did not. Goldsmith said he therefore reluctantly sent a detailed e-mail to Leitch on March 11 to support the Department's contention that it had properly informed the White House of Ashcroft's status. Goldsmith stated that in the e-mail he also made the point that his conversation with Gonzales on March 9, 2004 (discussed above) was premised on Gonzales's knowledge that Ashcroft was ill and that Comey needed to authorize a "30-day bridge" until Ashcroft was well enough to sign the Authorizations again.[167] (U)

Gonzales told us that he had no recollection of having seen OLC's March 5, 2004, memorandum entitled "Determination that Attorney General is absent or disabled." As described above, Gonzales stated that he and Card would not have gone to the hospital if they believed Ashcroft did not have the authority to certify the Authorization as to form and legality. Gonzales also said that while he believed Comey would be making the decision to recertify the program, this did not mean that Ashcroft had relinquished his authority or had been "recused" from making the decision. Gonzales said he believed that Ashcroft retained the authority if he was competent to exercise it and was inclined to do so.[168] ~~(TS//SI//NF)~~

---

memorandum from Comey's Chief of Staff Chuck Rosenberg memorializing Comey's decision that the Attorney General was "absent or disabled" within the meaning of 28 U.S.C. § 508(a). Leitch's clarification stated that the Rosenberg memorandum had been in draft form. (U)

[167] The OIG searched for but was unable to find this e-mail from Goldsmith to Leitch. (U)

[168] During his July 24, 2007, testimony before the Senate Judiciary Committee, however, Gonzales stated that he thought there had been newspaper accounts of Comey's assumption of the Attorney General's duties and stated that "the fact that Mr. Comey was the acting Attorney General is probably something that I knew of." Gonzales testified that he was aware that Ashcroft was ill and had undergone surgery, but Gonzales stated that Ashcroft "could always reclaim" his authority. (U)

7. March 11, 2004: Gonzales Certifies Presidential Authorization as to Form and Legality ~~(TS//SI//NF)~~

On the morning of March 11, 2004, with the Presidential Authorization set to expire, President Bush signed a new Authorization.[169] In a departure from the past practice of having the Attorney General certify the Authorization as to form and legality, the March 11 Authorization was certified by White House Counsel Gonzales. The March 11 Authorization also differed markedly from prior Authorizations in three other respects. ~~(TS//STLW//SI//OC/NF)~~

The first significant difference between the March 11, 2004, Presidential Authorization and prior Authorizations was the President's explicit assertion that the exercise of his Article II Commander-in-Chief authority "displace[s]the provisions of law, including the Foreign Intelligence Surveillance Act and chapter 119 of Title 18 of the United States Code (including 18 U.S.C. §2511(f) relating to exclusive means), to the extent of any conflict between the provisions and such exercises under Article II[.]" As discussed above, FISA and the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2521 (generally referred to as Title III) are by their terms the "exclusive means by which electronic surveillance, as defined in [FISA], and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f). This new language was based on the same legal rationale Yoo first advanced in support of the Stellar Wind program – that FISA cannot be read to infringe upon the President's Commander-in-Chief authority under Article II of the Constitution during wartime. ~~(TS//STLW//SI//OC/NF)~~

Subsequent Presidential Authorizations did not include this language discussing the legal bases for the program. Steven Bradbury told the OIG that he believed the language was included in the March 11 Authorization as a way of indicating that the President did not agree with Goldsmith and Philbin's analysis, and to protect those who had been implementing the program under the prior OLC opinions. ~~(TS//SI//NF)~~

Second, to narrow the gap between the authority given on the face of prior Authorizations and the actual operation of the program by the NSA, the terms governing the collection of telephony and e-mail meta data were clarified. The underlying language for "acquiring" both telephony and e-mail meta data remained as it had been, giving the NSA authority to:

---

[169] The March 11, 2004, Presidential Authorization stated that it would expire on May 6, 2004. ~~(TS//SI//NF)~~

> acquire, with respect to a communication, header/router/addressing-type information, including telecommunications dialing-type data, but not the contents of the communication, when (i) at least one party to such communication is outside the United States, (ii) no party to such communication is known to be a citizen of the United States, or (iii) based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are specific and articulable facts giving reason to believe that such communication relates to international terrorism, or activities in preparation therefor. ~~(TS//STLW//SI//OC/NF)~~

Presidential Authorization, March 11, 2004, para. 4(b). However, this language was now qualified by the following two subparagraphs:

> (i) the Department of Defense may obtain and retain header/router/addressing-type information, including telecommunications dialing-type data, (b)(1), (b)(3) [redacted] provided that search and retrieval from such obtained header/router/addressing-type information, including telecommunications dialing-type data, shall occur only in accordance with this authorization; and
>
> (ii) header/router/addressing-type information, including telecommunications dialing-type data, is "acquired" for purposes of subparagraph 4(b) above when, and only when, the Department of Defense has searched for and retrieved such header/router/addressing-type information, including telecommunications dialing-type data (and not when the Department obtains such header/router/addressing-type information, including telecommunications dialing-type data, such as (b)(1), (b)(3) [redacted] for retention).

Id. at para. 4(b)(i) & (ii). ~~(TS//STLW//SI//OC/NF)~~

In essence, the March 11, 2004, Authorization for the first time sought to make clear that the NSA could "obtain and retain" telephony and e-mail meta data (baskets 2 and 3) (b)(1), (b)(3) [redacted] but the meta data collected could only be queried ("acquired") in accordance with any of the three conditions set forth in paragraph 4(b).[170] This language clarifying what the term "acquire"

---

[170] The term "obtain," as first introduced in the March 11, 2004, Presidential Authorization, was meant to be synonymous with the term "collect." ~~(TS//SI//NF)~~

meant was included in every successive Presidential Authorization for the remainder of the program. ~~(TS//STLW//SI//OC/NF)~~

Moreover, the President asserted in the March 11 Authorization that the newly drafted distinction between "obtaining and retaining" meta data versus "acquiring" the meta data "reflects the consistent course of conduct under such Presidential Authorizations that has been known to and authorized by me, and shall be deemed to have been a part of such Presidential Authorizations as if [paragraph 4(b)(i) & (ii)] had been explicitly included in each such Presidential Authorization at the time of presidential signature; any action taken prior to presidential signature of this authorization that is consistent with the preceding sentence is ratified and confirmed."[171] Id. at para. 4(b). ~~(TS//STLW//SI//OC/NF)~~

According to Comey and Philbin, this new language was Addington's "fix."[172] Philbin said he believed the new language was "sufficient" to address the Department's concern that the Authorizations did not adequately describe the (b) (5), (b)(1), (b)(3) being carried out by the NSA, although he believed the new language was "cumbersome." (b) (5)

~~(TS//STLW//SI//OC/NF)~~

In his OIG interview, Gonzales declined to explain the significance of this new language, based on an assertion from the Special Counsel to the President that his answer would reveal internal White House deliberations. (b) (5), (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~

[171] (b)(1), (b)(3), (b) (5)

~~(TS//STLW//SI//OC/NF)~~

[172] Hayden and Philbin both told the OIG that Addington drafted the Presidential Authorizations. In his OIG interview, we asked Gonzales who drafted the March 11, 2004, Authorization. On the advice of the Special Counsel to the President, Gonzales declined to answer. ~~(TS//SI//NF)~~

The March 11 Presidential Authorization did not [redacted] (b)(1), (b)(3), (b)(5)

[redacted] (~~TS//STLW//SI//OC/NF~~)

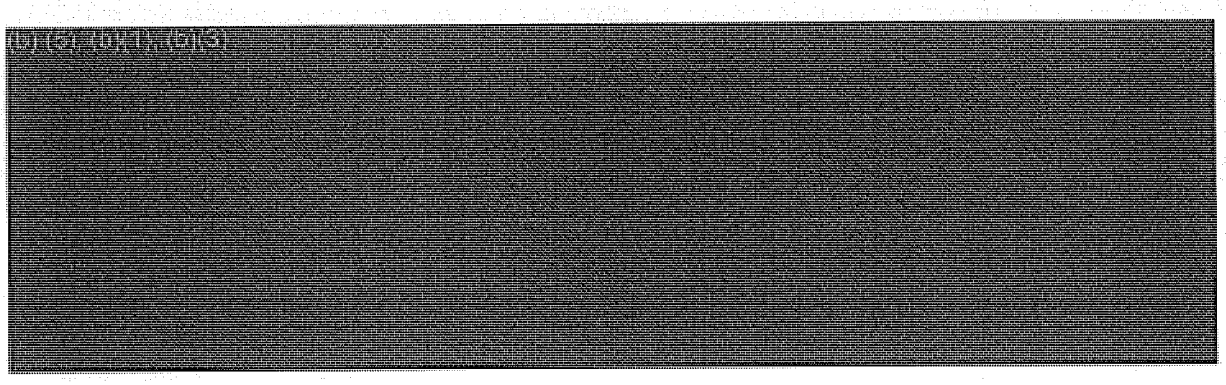
The third significant departure from prior Authorizations was the inclusion of a statement that "the Attorney General of the United States approved as to form and legality [all prior Presidential Authorizations] authorizing the same activities as are extended by this authorization[.]" Id. at para. 10. (~~TS//STLW//SI//OC/NF~~)

[redacted] (b) (5)

[redacted] (b) (5), (b)(3)

[redacted] (b) (5), (b)(1), (b)(3)

However, Gonzales told us that he found it "hard to believe" that no one at the Department understood that the NSA was [redacted] (b)(1), (b)(3) Gonzales said he was aware that Philbin had been to the NSA several times and had met with NSA officials to gain an understanding of how the program was actually implemented. (~~TS//STLW//SI//OC/NF~~)



We asked Gonzales why he signed the March 11, 2004, Presidential Authorization even though the Department could not support it. On the advice of the Special Counsel to the President, Gonzales declined to answer. However, Gonzales stated that the White House Counsel, like OLC, provides legal advice to the President and that his signature on the Authorization simply represented his advice as to its form and legality. ~~(TS//SI//NF)~~

NSA Director Hayden told us that Addington asked him whether the NSA would be willing to continue the Stellar Wind program without the Justice Department's certification of the Presidential Authorization. Hayden said this was a "tough question" and that he consulted with his leadership team at the NSA before making a decision. Hayden said that three considerations persuaded him to continue the program. First, the congressional members briefed on the situation on March 10, 2004, were supportive of continuing the program without Comey's certification. Second, the program had been operating for the previous two and a half years with Department approval. Third, the NSA General Counsel's office told him the program was legal. Hayden said he was unsure whether proceeding without the Department's certification was a sustainable approach, but that he was comfortable doing so when the issue arose in March 2004. ~~(TS//SI//NF)~~

B. Department and FBI Officials React to Issuance of March 11, 2004, Authorization ~~(TS//SI//NF)~~

Several Department and FBI leadership officials considered resigning after the Presidential Authorization was signed despite the Deputy Attorney General's refusal to certify the program based on the Department's determination that certain activities it authorized were without adequate legal support. Many of the Department, FBI, and White House officials we interviewed characterized the events immediately surrounding the issuance

---

[174] In a closed session of the Senate Select Committee on Intelligence on June 26, 2007, Comey described his belief regarding the new language, stating, "[T]here were some additions to the text that were an effort by someone to try and fix the record in some respect." (U//~~FOUO~~)

of the March 11, 2004, Presidential Authorization in dramatic, sharp terms. Several of the Department witnesses described the impasse as a "crisis" and described a sense of distrust and anger that permeated their relations with White House officials during this period. In a letter of resignation that Comey wrote but did not send, he described this period as an "apocalyptic situation." ~~(TS//SI//NF)~~

In this section, we describe the reactions of Department, FBI, and White House officials to the White House decision to continue the program without the support of the Justice Department. (U)

1. Initial Responses of Department and FBI Officials (U)

White House Chief of Staff Card informed Comey by telephone on the morning of March 11, 2004, that the President had signed the new Authorization that morning. At approximately noon, Gonzales called Goldsmith to inform him that the President, in issuing the Authorization, had made an interpretation of law concerning his authorities and that the Department should not act in contradiction of his determinations. Goldsmith took notes on the call. According to his notes, Goldsmith asked Gonzales, "What were those determinations?" and Gonzales responded that he would let Goldsmith know. ~~(TS//SI//NF)~~

Later that day, Gonzales called Goldsmith again and told him that OLC should continue working on its legal analysis of the program. In a third call that day, however, Gonzales directed Goldsmith to suspend work on the legal analysis and to decline a request from the CIA General Counsel to review a draft of the new OLC memorandum. ~~(TS//SI//NF)~~

Goldsmith followed up this series of calls with a letter to Gonzales seeking clarification on Gonzales's instructions. Goldsmith wrote that he interpreted the March 11, 2004, Authorization signed by the President to mean that "the President has determined the legality of [the program] in all respects based upon the advice and analysis of your office, and that officers of the Department of Justice should refrain from calling into question the legality of [the program], or from undertaking further legal analysis of it." In the letter Goldsmith recounted how Gonzales had then called him to advise that OLC should continue its legal analysis of the program, adding, "I am now uncertain about your direction based on the President's exercise of his authority." Goldsmith concluded his letter by reiterating OLC's position that its existing legal memoranda "should not be relied upon in support for the entire program." Goldsmith described the document he wrote as a "for the record" letter.[175] As described below, Goldsmith and Philbin delivered

[175] Goldsmith said he discussed a draft of the letter with Comey, Rosenberg, Ayres, Olson, and others and edited it based on their suggestions. (U)

this letter to Gonzales at his residence at approximately 11:00 p.m. that night. ~~(TS//SI//NF)~~

At noon on March 11, 2004, Director Mueller met with Card at the White House. According to Mueller's program log, Card summoned Mueller to his office to bring Mueller up to date on the events of the preceding 24 hours. Card recounted for Mueller the briefing of the congressional leaders the prior afternoon and the President's issuance of the new Authorization without the Department's approval. In addition, Card told Mueller that if no "legislative fix" could be found by May 6, 2004, when the current Authorization was set to expire, the program would be discontinued. ~~(TS//SI//NF)~~

According to Mueller's notes, Card acknowledged to Mueller that President Bush had sent him and Gonzales to the hospital to seek Ashcroft's certification for the March 11, 2004, Authorization, but that Ashcroft had said he was too ill to make the determination and that Comey was the Acting Attorney General. Mueller wrote in his program log that he told Card that the failure to have Department of Justice representation at the congressional briefing and the attempt to have Ashcroft certify the Authorization without going through Comey "gave the strong perception that the [White House] was trying to do an end run around the Acting [Attorney General] whom they knew to have serious concerns as to the legality of portions of the program." Card responded that he and Gonzales were unaware at the time of the hospital visit that Comey was the Acting Attorney General, and that they had only been following the directions of the President. ~~(TS//SI//NF)~~

Mueller reminded Card that Mueller had told Vice President Cheney during their March 9, 2004, noon meeting that Mueller could have problems with the FBI's continued involvement in the program if the White House issued an Authorization without the Department's approval. Card said he understood Mueller's concern and told him to stop by Gonzales's office to pick up a copy of the March 11, 2004, Authorization, which Mueller did. ~~(TS//SI//NF)~~

Mueller met with Comey at 1:15 p.m. to review the Authorization, and he left a copy of it with Comey. During this meeting, Mueller told Comey he would be submitting a letter to Comey requesting advice on the legality of the FBI's continued participation in the program.[176] ~~(TS//SI//NF)~~

[176] According to the Mueller's program log, Gonzales called Mueller at 2:50 p.m. to tell him to "assure security of copy of President's order." (U)

Later that day, Mueller sent Comey a memorandum, prepared by FBI General Counsel Valerie Caproni and an FBI Deputy General Counsel, seeking guidance on how the FBI should proceed in light of recent developments. The memorandum asked whether FBI agents detailed to the NSA to work on Stellar Wind should be recalled; whether the FBI should continue to receive and investigate tips based on [redacted] and whether [redacted] ~~(TS//STLW//SI//OC/NF)~~

Office of Intelligence Policy and Review (OIPR) Counsel James Baker also expressed his concern about the White House's action. On the evening of March 11, 2004, he drafted a memorandum to Comey containing what he later described as a series of "loaded questions" concerning whether it was "lawful and ethical" for OIPR to continue filing applications with the FISA Court under the circumstances.[177] ~~(TS//SI//NF)~~

Goldsmith and Philbin called Gonzales late in the evening of March 11 to ask if they could visit him at his residence to deliver the letter Goldsmith had written earlier in the day. As described above, Goldsmith sought to make a record of his earlier conversations with Gonzales in which Goldsmith believed Gonzales had conveyed conflicting instructions regarding how OLC should proceed in light of the President's issuance of the March 11 Authorization. ~~(TS//SI//NF)~~

Gonzales told us that Goldsmith drafted the letter because Goldsmith was "confused" about whether OLC should continue working on its legal analysis of the program. Gonzales said he recalled that Goldsmith and Philbin were "somber" during the meeting at his house. Gonzales said that he told them that the President had decided to go forward with the program, but that they should continue working to resolve the outstanding legal questions they had and try to find a solution. He said he tried to convey to them his confidence that everyone would "get through this." ~~(TS//SI//NF)~~

Goldsmith and Philbin told us that Gonzales was very cordial during the meeting and expressed regret for having gone to Ashcroft's hospital room that evening. Philbin stated that initially he believed that Gonzales had instructed him and Goldsmith "not to do our job, not to determine what the law is," but that it became evident to him that Gonzales "wanted to do the legally right thing." Goldsmith also stated that as a general proposition

---

[177] These issues are described in Section II C of this chapter in connection with the Department's meetings with FISA Court Presiding Judge Kollar-Kotelly to discuss the use in FISA applications of information derived from [redacted] collected under the program following the March 11, 2004, Presidential Authorization and its subsequent modifications. ~~(TS//STLW//SI//OC/NF)~~

he encountered more "pushback" from Addington than from Gonzales, and that Gonzales "wanted to do the right thing." ~~(TS//SI//NF)~~

2. Department and FBI Officials Consider Resigning (U)

Comey told us he drafted a letter of resignation shortly after the incident in Ashcroft's hospital room on March 10. Comey said he drafted the letter because he believed it was impossible for him to remain with the Department if the President would do something the Department said was not legally supportable.[178] (U)

Comey also testified that Ashcroft's Chief of Staff David Ayres believed Ashcroft also was likely to resign and urged Comey to wait until Ashcroft was well enough to resign with him. In written responses to Senator Charles Schumer following his testimony, Comey wrote that he believed the following individuals also were prepared to resign: Goldsmith, Philbin, Chuck Rosenberg, Daniel Levin, James Baker, David Ayres, Deputy Chief of Staff to the Attorney General David Israelite, and Director Mueller. Comey also responded to the question that he believed that "a large portion" of his staff also would have resigned if he had. (U)

Goldsmith told us he was "completely disgusted" by his recent meetings with White House officials in connection with the Stellar Wind program and that he drafted a resignation letter at around the same time as Comey. The OIG obtained a handwritten list Goldsmith had compiled as these events were taking place to memorialize his grievances with the White House's actions during this period. The list includes:

- the "[s]hoddiness of the whole thing," which Goldsmith told us referred to his belief that both the process by which the program was implemented and the substantive analysis underpinning it represented the extreme opposite of how to manage a program as important as the White House claimed Stellar Wind to be;

---

[178] The letter was addressed to President Bush. Also, at 5:46 p.m. on the evening of March 11, 2004, Comey sent an e-mail to two Department colleagues stating in part:

> I have been through the roughest patch of my professional life in the last 24 hours. You would not believe what has gone on . . . . I am hugely upset about the conduct of certain members of the executive branch. But I am also hugely proud of the Department of Justice, including SG, Associate AG, OLC, Ayres, my staff, the AG, and even Mrs. Ashcroft. I believe this has been our finest hour, although it is not over yet. . . . I suspect I will either be fired by the President or quit, but I will have done the right thing for my country. (U)

- "[o]ver-secrecy," both in terms of not reading in attorneys at the Justice Department and other agencies, and not keeping Congress informed;
- the hospital incident, which Goldsmith described as "shameful"; "[d]isregard of law" on the part of the White House (a reference Goldsmith did not expand upon with more specificity during his interview with the OIG); and
- the White House's claim that a legislative fix could be achieved, which Goldsmith regarded as "irresponsible" because he believed at the time that a legislative remedy was not a viable option. ~~(TS//SI//NF)~~

Goldsmith described three additional items on the list in particular as "false representations" by the White House:

- "[l]ies re shutting down," referring to the White House's assurances to Goldsmith on several occasions that it would shut down the program if the Office of Legal Counsel could not find legal support for it;
- "[l]ies re telling [the President] of problem," referring to representations that the President had been kept informed of the Department's concerns about the program; and
- assertions by White House officials that they "[d]idn't know AG was incapacitated". ~~(TS//SI//NF)~~

Goldsmith stated that on Thursday, March 11, Ayres asked him not to resign because the Attorney General should have the chance to do so first once he had fully recovered from his surgery. Goldsmith said he was still "on the fence" the following Monday or Tuesday about resigning and that there was great concern that his and other resignations would "spark a panic" that might lead to the program being revealed publicly.[179] (U)

Philbin told us that there was an "eerie silence" at the Department on March 11 as he and others awaited word from the White House on the fate of the program. Philbin said he and others believed they would have to resign. Philbin said his primary concern was that the White House planned to go forward with the Presidential Authorization and continue the program

[179] Goldsmith ultimately tendered his resignation in June 2004, effective July 30, 2004. Goldsmith told us he resigned in part because he did not believe he could be an effective head of the Office of Legal Counsel after his "unprecedented" withdrawal of several legal memoranda, including those drafted by Yoo. Goldsmith added that he also resigned because he was "exhausted" from his work in OLC and had recently been offered a teaching position at Harvard Law School. (U)

despite the flaws that the Office of Legal Counsel had identified in its legal analysis. Philbin said he was "absolutely serious" about resigning, adding, "[If] they're going to try to strong-arm the guy on morphine, what else are they going to do?" ~~(TS//SI//NF)~~

Baker told us that he also considered resigning after the President signed the Authorization but ultimately decided to remain in his position, in part because of his fear that if the White House was willing to tolerate mass resignations of senior government officials rather than revise the Stellar Wind program, "I don't know what this means in terms of the rule of law in this country." Baker also stated that he knew he had certain protections from removal for a period of time because he was a career official and that he wanted to remain as Chief of OIPR to protect the government's relationship with the FISA Court and to protect the attorneys in his office. ~~(TS//SI//NF)~~

Levin said he was willing to resign over the matter, and he gave a signed resignation letter to Comey to be used by him "however [he] felt appropriate." Levin said he did so "if it would help to get the White House to change its mind." Levin said that even though he was not certain he shared Goldsmith's view that the [redacted] was legally without support, he thought the White House's conduct during the incident at the hospital had been "outrageous" and he was willing to resign on that basis alone. ~~(TS//STLW//SI//OC/NF)~~

FBI General Counsel Caproni told us that she also was prepared to resign. She said that the FBI's primary concern regarding the impasse between the Department and the White House over the program was not with issues of privacy and civil liberties, but rather with "the rule of law." ~~(TS//SI//NF)~~

At approximately 1:30 a.m. on March 12, 2004, Mueller drafted by hand a letter stating, in part: "[A]fter reviewing the plain language of the FISA statute, and the order issued yesterday by the President . . . and in the absence of further clarification of the legality of the program from the Attorney General, I am forced to withdraw the FBI from participation in the program. Further, should the President order the continuation of the FBI's participation in the program, and in the absence of further legal advice from the AG, I would be constrained to resign as Director of the FBI." Mueller told us he planned on having the letter typed and then tendering it, along with his March 11, 2004, memorandum to Comey, but that based on subsequent events his resignation was not necessary. ~~(TS//SI//NF)~~

3. Comey and Mueller Meet with President Bush (U)

On the morning of March 12, 2004, Comey and Mueller went to the White House to attend the regular daily threat briefing with the President in the Oval Office. Comey said that following the briefing President Bush called him into the President's private study for an "unscheduled meeting." (U)

Comey told us that President Bush said to him, "You look burdened." Comey told the President that he did feel burdened, to which the President responded, "Let me lift that burden from you." Comey told the President that he felt as if he were standing on railroad tracks with a train coming toward him to run over his career and "I can't get off the tracks." (U)

Comey said he then explained to the President the three baskets of Stellar Wind collection and the issues and problems associated with each. President Bush responded with words to the effect, "You whipped this on me" all of a sudden, that he was hearing about these problems at the last minute, and that the President not being told of these developments regarding the program was "not fair to the American people." Comey responded that the President's staff had been advised of these issues "for weeks," and that the President was being "poorly served" and "misled" by his advisors. Comey also said to the President, "The American people are going to freak when they hear what collection is going on." President Bush responded, "That's for me to worry about." ~~(TS//STLW//SI//OC/NF)~~

According to Comey, the President said that he just needed until May 6 (the date of the next Authorization), and that if he could not get Congress to fix FISA by then he would shut down the program. The President emphasized the importance of the program and that it "saves lives." Comey told the President that while he understood the President's position he still could not agree to certify the program. Comey said he then quoted Martin Luther to the President: "Here I stand, I can do no other." At the end of the conversation, Comey told the President, "You should know that Bob Mueller is going to resign this morning." The President thanked Comey for telling him that and said he would speak with Mueller next. ~~(TS//STLW//SI//OC/NF)~~

Comey said his conversation with the President lasted approximately 15 minutes. Following the conversation, Comey went to Mueller, who was waiting in the West Wing, and started discussing his meeting with the

President. Word was then sent to Mueller through a Secret Service agent that the President wanted to meet with him.[180] (U)

Mueller later made notes in his program log about his meeting with President Bush. According to his notes, the President told Mueller that he was "tremendously concerned" about another terrorist attack and that he had been informed that the Stellar Wind program was essential to protecting against another attack. The President cited an ongoing investigation [redacted] The President said he believed that he would be "justly held accountable" if he did not do everything possible to prevent another attack. The President explained to Mueller that for these reasons he had authorized the continuation of the program even without the concurrence of the Attorney General as to the legality of "various aspects of the program." ~~(TS//STLW//SI//OC/NF)~~

b1, b3, b7E

According to the notes, the President told Mueller that the congressional leadership had been briefed on the President's action to extend the program and was "understanding and supportive of the President's position." The President also told Mueller that he had urged Comey to agree to extend the program until May 6 and that he hoped for a legislative fix by that time, but that if no legislative solution could be found and the legality of the program was still in question by that time, he "would shut it down." ~~(TS//SI//NF)~~

According to Mueller's notes, Mueller told the President of his concerns regarding the FBI's continued participation in the program without an opinion from the Attorney General as to its legality, and that he was considering resigning if the FBI were directed to continue to participate without the concurrence of the Attorney General. The President responded that he "wished to relieve any burden [Mueller] may be laboring under" and that he did not want Mueller to resign. Mueller said he explained to the President that he had an "independent obligation to the FBI and to the Justice Department to assure the legality of actions we undertook, and that a presidential order alone could not do that." ~~(TS//SI//NF)~~

---

[180] At this point (9:27 a.m.), Comey sent an e-mail from his Blackberry to Goldsmith, Philbin, Ayres, Levin, and others, stating:

> President just took me into his private office for 15 minute one on one talk. Told him he was being misled and poorly served. We had a very full and frank exchange. Don't know that either of us can see a way out. He promised that he would shut down 5/6 if Congress didn't fix FISA. Told him Mueller was about to resign. He just pulled Bob into his office.
> ~~(TS//SI//NF)~~

According to Mueller's notes, the President expressed understanding for Mueller's position and asked what needed to be done to address Mueller's concerns. Mueller responded that Comey, the Office of Legal Counsel, the CIA, and the NSA "needed to sit down immediately" and assess the legal status of the program in light of OLC's doubts about the existing legal rationale and the March 11, 2004, Authorization. Mueller wrote:

> The President questioned me closely on the impact on national security from discontinuing elements of the program. [redacted]

According to Mueller's notes, the President then directed Mueller to meet with Comey and other principals to address the legal concerns so that the FBI could continue participating in the program "as appropriate under the law." ~~(TS//SI//NF)~~

Mueller told us he met with Comey an hour later to begin coordinating that effort. At 4:50 p.m. that afternoon, Mueller called Gonzales to request that additional Department lawyers be read into the program.[181] Mueller told us that this request originated with Comey and that Mueller was merely acting as an "intermediary." (U)

The President's direction to Mueller to meet with Comey and other principals to address the legal concerns averted the mass resignations at the Department and the FBI. According to Comey and other Department officials, the White House's decision to seek a legal solution and allow more attorneys to be read into the program was a significant step toward resolving the dispute, and in the words of one Department official provided a way of "stepping back from the brink." As we describe below, these Department officials still faced the challenge of finding a legal and operational remedy for the program that would address the concerns of the White House, the NSA, and Department. ~~(TS//SI//NF)~~

4. Comey Directs Continued Cooperation with NSA (U)

On the morning of March 12, 2004, Comey decided not to direct OIPR and the FBI to cease cooperating with the NSA in conjunction with the program. Comey's decision is documented in a 1-page memorandum from

[181] At least three additional Department attorneys were read into the program on March 12, 2004, including OIPR Acting Deputy Counsel for Intelligence Operations Peggy Skelly-Nolen and two OLC attorneys. (U)

Goldsmith to Comey in which Goldsmith explained why Comey's action was legal. ~~(S//NF)~~

In his memorandum, Goldsmith stated that the President, as Commander-in-Chief and Chief Executive with the constitutional duty to "take care that the laws are faithfully executed," made a determination that Stellar Wind, as practiced, was lawful. Goldsmith concluded that this determination was binding on the entire Executive Branch, including Comey in his exercise of the powers of the Attorney General.[182] ~~(TS//SI//NF)~~

(b)(5)

[redacted]

5. Department Conducts Additional Legal Analysis (U)

On March 12, 2004, an interagency working group was convened to continue the legal analysis of the program. In accordance with the President's directive to Mueller, officials from the FBI, NSA, and the CIA were brought into the process, although the OLC maintained the lead role. The working group included Deputy Solicitor General Clement, Baker, FBI General Counsel Caproni, Mueller, and several attorneys from OLC. Comey said CIA Director Tenet and his Deputy, McLaughlin, may have had limited participation as well. ~~(TS//STLW//SI//OC/NF)~~

On March 13, Mueller asked NSA Director Hayden to assist FBI General Counsel Caproni in assessing the value of the Stellar Wind program. Mueller said he wanted Caproni to become more familiar with the program and to understand how the FBI's view of the value of the program

[182] Goldsmith told us his determination that the entire Executive Branch was bound by the President's interpretation of law was based on his discussions with several other Justice Department attorneys, as well as on long-standing OLC precedent. (U)

compared with that of the NSA.[183] Mueller said that Hayden provided slides highlighting cases in which the NSA believed Stellar Wind-derived information proved useful. ~~(S//NF)~~

Caproni told us that during this March 2004 period she and two other FBI officials made an effort to determine what value the FBI was getting from Stellar Wind-derived information. She explained that it was difficult to assess the value of the program during its early stages because FBI field offices at that time were not required to report back to FBI Headquarters with information about how information from the NSA program had been used.[184] ~~(S//NF)~~

On the afternoon of Sunday, March 14, 2004, the Department convened a large meeting in the Justice Command Center to review OLC's analysis on the legality of the program. Mueller, Comey, Goldsmith, Philbin, Baker, CIA General Counsel Muller, Caproni, Tenet, Hayden, Olson, Clement, and several NSA lawyers attended the meeting. ~~(TS//SI//NF)~~

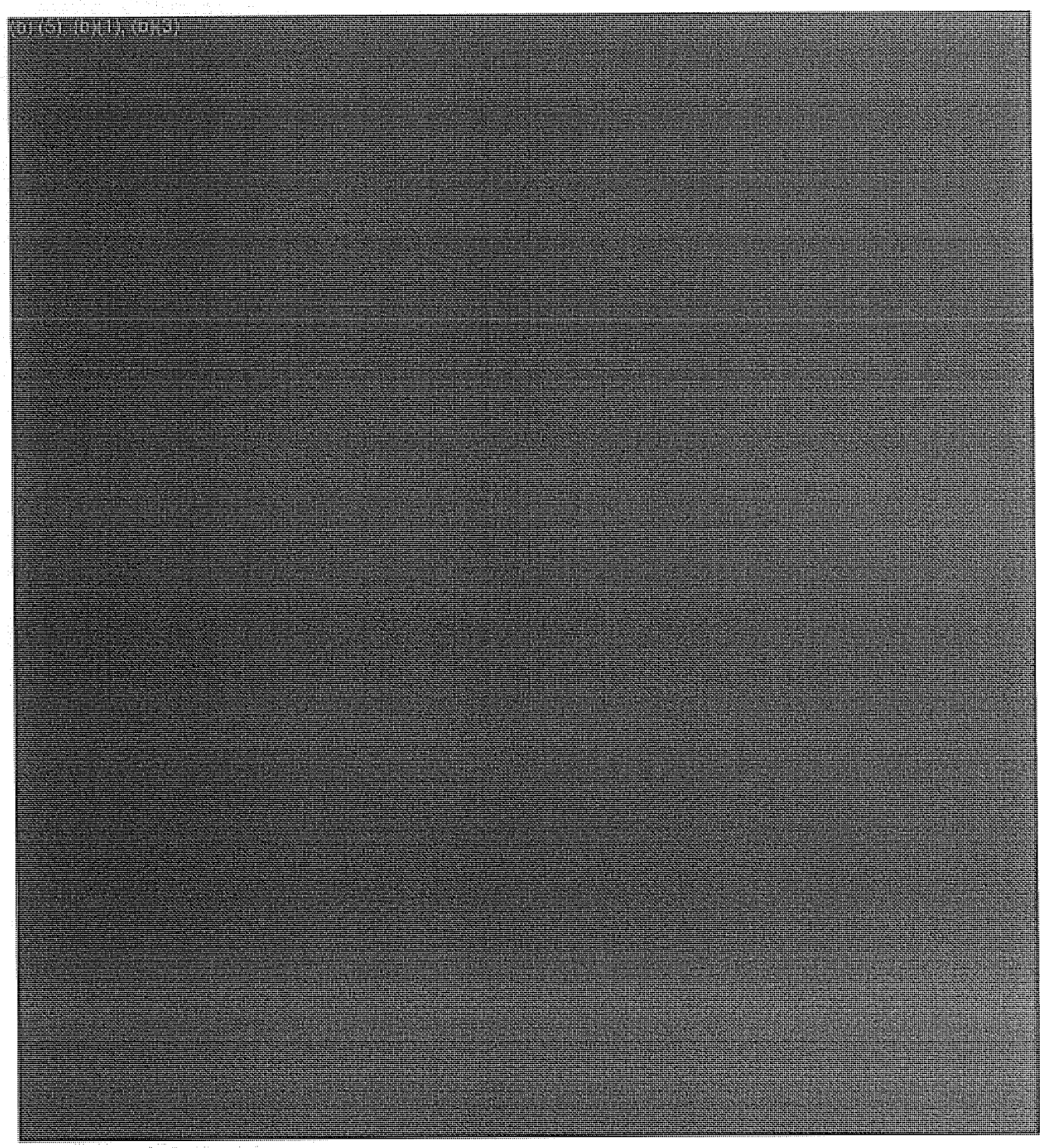
Prior to the meeting, Goldsmith and Philbin prepared a detailed outline of OLC's current analysis, which Goldsmith described to us as his "most honest take" of the legal issues at that time. Goldsmith said he distributed the outline to meeting participants and used it to walk the group through the analysis. (U)

The outline highlights the evolution of OLC's analysis. (b)(3), (b)(1), (b)(3)

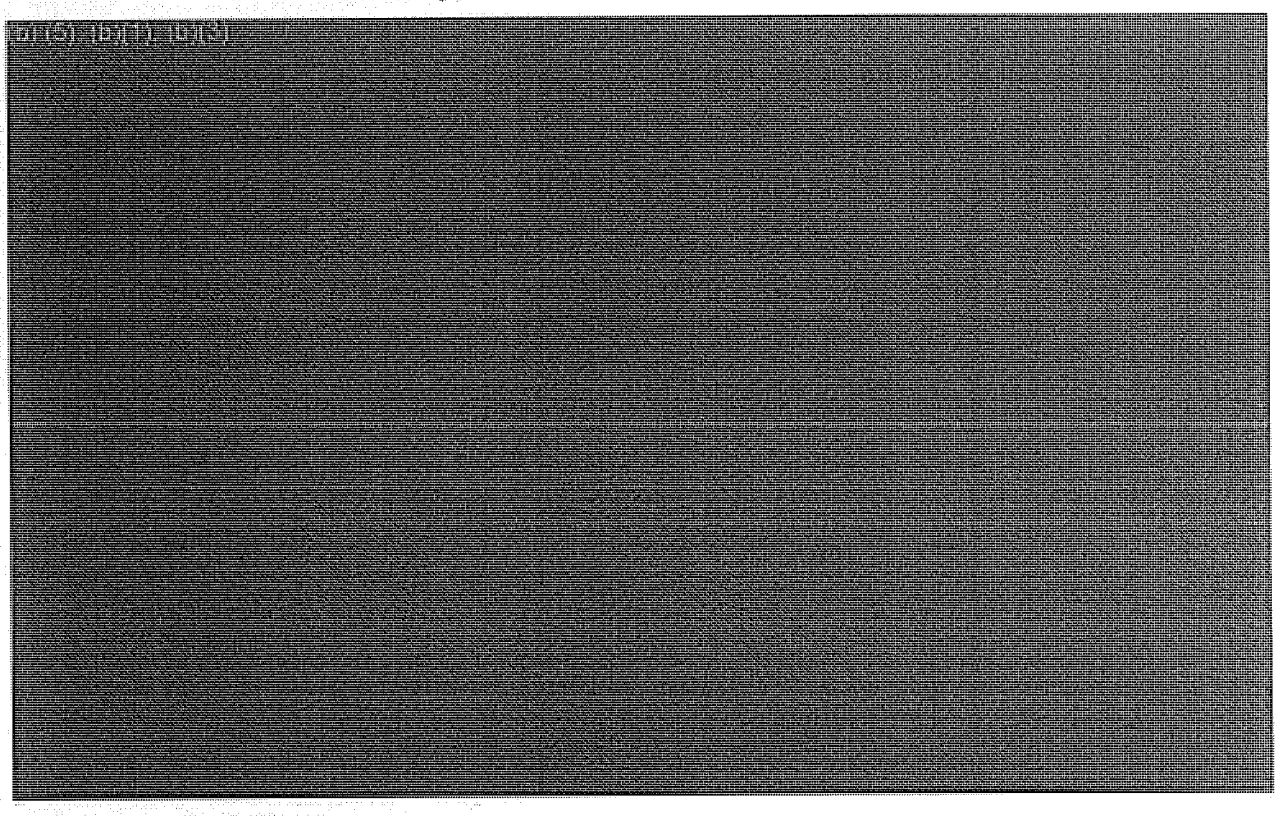
[redacted]

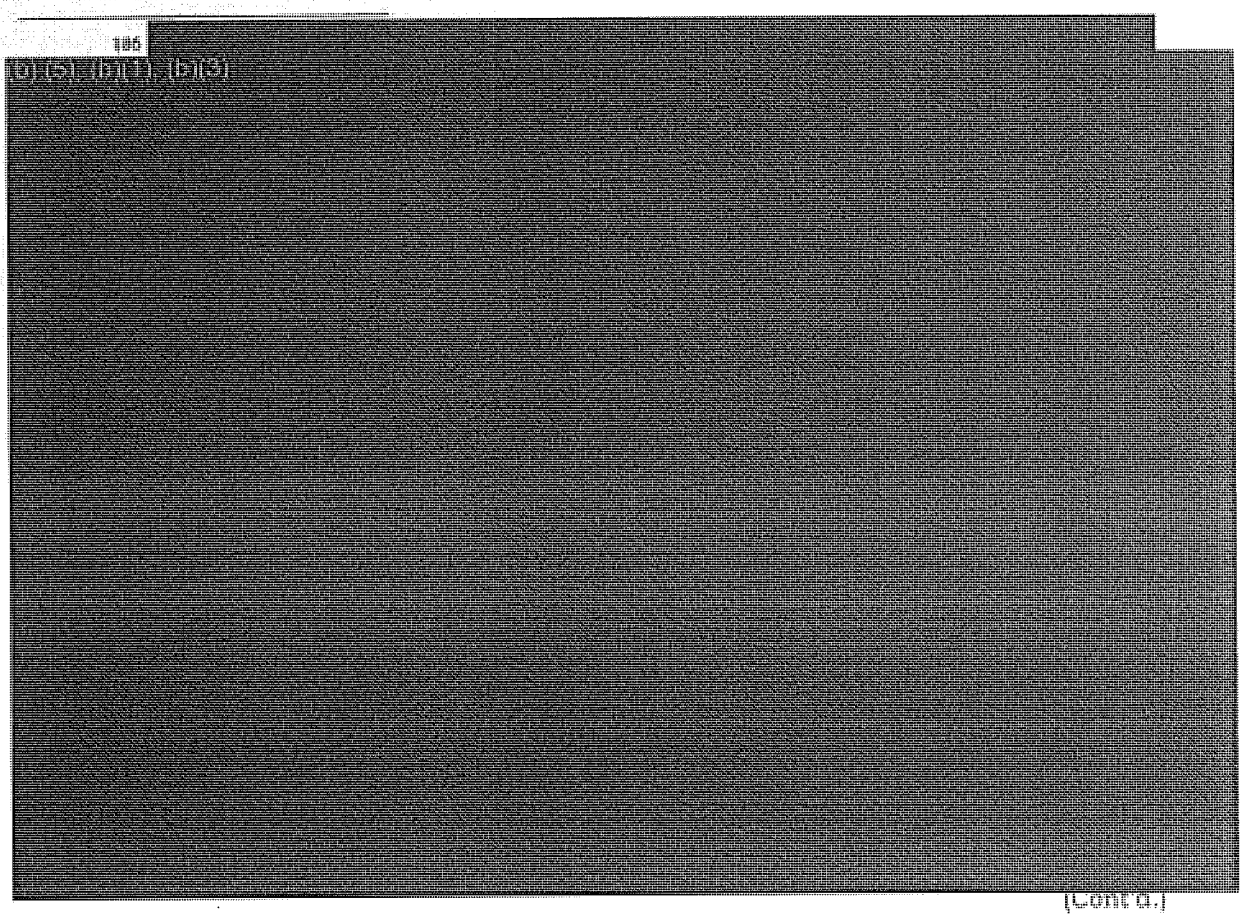
[183] Caproni had been appointed the FBI General Counsel in August 2003 and was read into the Stellar Wind program in September or October 2003. She told us she did not give much thought to the program at the time because OLC had determined that it was legal. She stated that in 2004 she learned that OLC was re-examining Yoo's legal analysis and had concerns with it. She told us she later spoke with Philbin, who confirmed to her that he and Goldsmith had problems with the legal support for the program and that he was frustrated because the program was so tightly compartmented that he could not talk to anybody about it. Caproni told us that at some point she obtained a copy of Yoo's legal opinion. She stated that after reading it she immediately understood Philbin's concerns because the opinion appeared to lack analysis and simply concluded that the program was legal. ~~(TS//SI//NF)~~

[184] The FBI's Electronic Communications Analysis Unit compiled a summary of known (b)(1), Stellar Wind tip results from January 1, 2003, through mid-December 2003. However, the data included in the summary was incomplete, and the summary did not contain any analysis of the effectiveness of these tips. Another study of the (b)(1), (b)(3) tippers was conducted in 2006. The results of that study are discussed in Chapter Six of this report, along with the OIG's analysis of the effectiveness of the program. ~~(TS//STLW//SI//OC/NF)~~ b1, b3



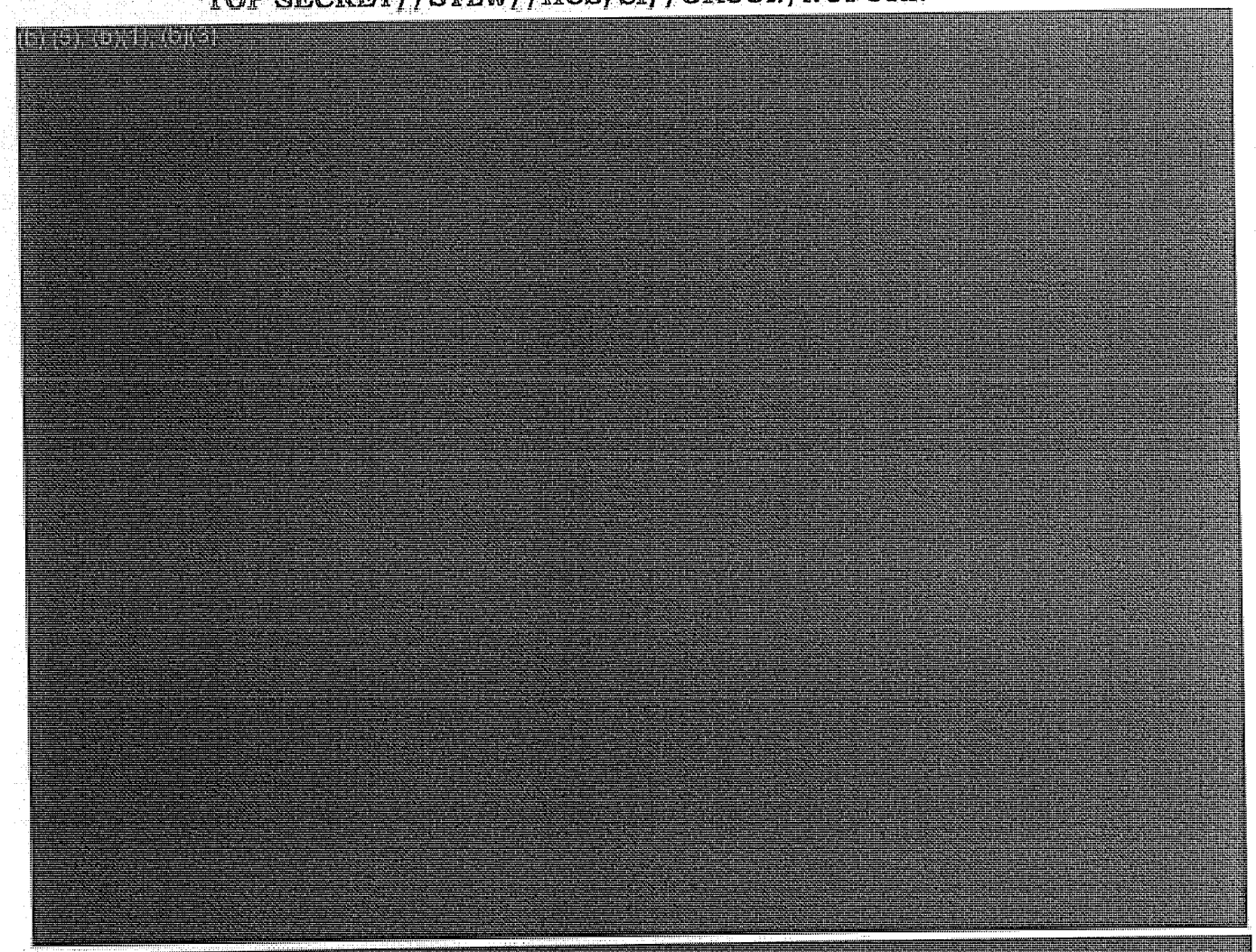
[185] Goldsmith also noted that as of the March 14, 2004, meeting, the Attorney General had not yet reported to Congress on the program under 28 U.S.C. § 530D. However, as discussed above, the White House had briefed the congressional leadership about the program on March 10, 2004. In addition, the former Presiding Judge of the FISA Court, Royce Lamberth, and the current Presiding Judge, Colleen Kollar-Kotelly, had been read into the program by this time. (U)





[Cont'd.]

(b) (5), (b) (1), (b) (3)



(b) (5), (b) (1), (b) (3)

[redacted]

Goldsmith told us that during his presentation of the legal analysis at the March 14 meeting he received "tough but fair and appropriate" questions from Mueller and Olson with respect to why the [redacted] (~~TS//STLW//SI//OC/NF~~)

Goldsmith told us that the March 14 meeting was designed to achieve full consensus among the principals on the issues, and that the meeting was successful in this regard. (U)

That evening, Mueller called Gonzales to report that progress had been made, although legal support for [redacted] still had not been found. Mueller also told Gonzales that in the future Gonzales should speak directly with Comey on these matters. ~~(TS//STLW//SI//OC/NF)~~

6. Comey Determines that Ashcroft Remains "Absent or Disabled" (U)

Attorney General Ashcroft was released from the hospital at noon on March 14, 2004. The next day, Comey advised Ayres by memorandum that Ashcroft's doctor believed that Ashcroft required additional time to recuperate at home and was not yet ready to resume his responsibilities as Attorney General. Comey's memorandum noted that the doctor intended to reassess Ashcroft's condition on March 24, 2004. Comey's memorandum stated that, based on these circumstances, Comey continued to believe that Ashcroft was "absent or disabled" within the meaning of 28 U.S.C. § 508(a). Comey's memorandum concluded:

> As before, notwithstanding my continued temporary capacity as Acting Attorney General, I intend, where possible, to exercise "all the power and authority of the Attorney General" pursuant to the authority that 28 C.F.R. § 0.15(a) delegates to me in my regular capacity as Deputy Attorney General. (U)

A copy of the memorandum was sent to Gonzales at the White House and to senior Department officials.[189] (U)

7. Judge Kollar-Kotelly Briefed on Lack of Attorney General Certification (U)

As discussed earlier in this report, the extent to which OIPR could use Stellar Wind-derived information in FISA applications had been limited by Judge Kollar-Kotelly, the FISA Court's Presiding Judge. After her read-in to the program in May 2002, Judge Kollar-Kotelly had directed OIPR to continue, with some modifications, the "scrubbing" procedures for FISA applications in place at that time. ~~(TS//STLW//SI//OC/NF)~~

According to an OLC memorandum, on March 14, 2004, Judge Kollar-Kotelly was informed that the President had reauthorized the Stellar Wind program, but that the latest Authorization lacked the Attorney General's certification as to form and legality.[190] The memorandum indicated that as a result of Judge Kollar-Kotelly's uncertainty about the implications of this development, she intended to insist on a complete separation of any information derived from Stellar Wind, whether directly or indirectly, from all FISA applications presented to the FISA Court. The memorandum noted that "[b]ecause of the way tips get worked into (and lost in) the mix of intelligence information, that standard would have virtually crippled all counter-terrorism FISAs." ~~(TS//STLW//SI//OC/NF)~~

8. Comey and Gonzales Exchange Documents Asserting Conflicting Positions (U)

According to Mueller's program log, on the morning of Monday, March 15, 2004, following the daily threat briefing in the White House Situation Room, President Bush remarked to Mueller that he understood "progress had been made," referring to the discussions on the legal basis for the Stellar Wind program. Mueller called Comey shortly thereafter to convey the President's remark. Mueller suggested to Comey that additional briefings on the program should be given to Congress, including to both the House and Senate Judiciary Committees. ~~(TS//SI//NF)~~

Also on March 15, Goldsmith drafted for Comey a 3-page memorandum summarizing OLC's views with respect to the legality of the program. The memorandum recast in narrative form Goldsmith's outline of

---

[189] As discussed below, Ashcroft's doctors later cleared Ashcroft to resume his duties as Attorney General as of March 31. (U)

[190] The memorandum was prepared in anticipation of a briefing for the Attorney General on March 30, 2004. (U)

March 14, 2004 (discussed above), and noted that OLC had not reached any "final conclusions and [was] not yet prepared to issue a final opinion on the program." The memorandum also stated that the Stellar Wind program potentially implicated various congressional and intra-Executive Branch reporting requirements imposed both by statute and Executive Order. The memorandum stated that OLC was only beginning to analyze these reporting issues. ~~(TS//SI//NF)~~

Goldsmith and Philbin went to see Gonzales on the afternoon of March 15 to explain what OLC had determined in its legal analysis to that point, and also to notify Gonzales that he would be hearing from Comey shortly about the Department's position as to the program's legality. (U)

According to Philbin's contemporaneous notes on the events of the next two days, on March 16, 2004, following the morning threat briefing at the White House, Comey told President Bush that OLC had finished its preliminary legal analysis of the program.[191] Comey asked the President if Comey should convey the details of the analysis to Gonzales, and the President indicated that Comey should do so. ~~(TS//SI//NF)~~

After Comey returned to the Department, he signed a short memorandum to Gonzales that he had drafted the night before. In the memorandum, Comey first recounted how the President on March 12, 2004, had directed the Justice Department to continue its analysis of the Stellar Wind program and to "provide its best advice concerning ways to change the program to conform with the Justice Department's understanding of the applicable law." Comey then described the composition of the working group convened to accomplish this objective and how the group's efforts had resulted in Goldsmith's 3-page analysis, which Comey attached to his memorandum. ~~(TS//SI//NF)~~

Comey then set out his advice to the President. According to the memorandum, Comey advised that the President may lawfully continue (b)(1), (b)(3) [redacted] Comey wrote that (b)(1), (b)(3) [redacted] involved "close legal questions, requiring legally aggressive – indeed, novel – supporting arguments . . . ." Comey further wrote that the Department remained unable to find a legal basis to support (b)(1), (b)(3) [redacted] Accordingly, Comey advised that such (b)(1), (b)(3) [redacted]

[191] Philbin told the OIG he kept notes of these events because Comey had asked him to "keep a record." (U)

(b)(1), (b)(3) Finally, Comey cautioned that he believed the ongoing collection of (b)(1), (b)(3) raised "serious issues" about congressional notification, "particularly where the legal basis for the program is the President's decision to assert his authority to override an otherwise applicable Act of Congress." Comey wrote that the Department would continue to explore the notification issue. ~~(TS//STLW//SI//OC/NF)~~

Comey instructed Goldsmith and Philbin to hand deliver the memoranda to Gonzales at the White House, which they did. Philbin also delivered copies to Solicitor General Olson. Philbin's notes indicate that Olson was "annoyed" that Comey had sent the memoranda to the White House without consulting him, and asked Philbin several times, "What's my role supposed to be here?" Olson also said to Philbin that he thought the memoranda were a "poke in the eye" to the White House. Philbin wrote that Olson's reaction "raised concerns that [Comey] may have gotten himself too far out there alone" by not bringing Olson in on the Department's legal opinion in advance. (U)

Comey told us that he knew his memorandum would anger people at the White House because he had put in writing the arguments questioning the legality of aspects of the program and that the memorandum and Goldsmith's attachment would become a part of the Presidential records and would be discovered later by historians. He stated he believed it was important to "make a record." (U)

According to Mueller's program log, Gonzales called Mueller at 1:45 p.m. on March 16 to discuss the situation. Gonzales explained to Mueller that, in view of the Department's tentative conclusion that legal support for (b)(1), (b)(3) was still lacking, Gonzales would have to make a recommendation to the President on how to proceed. Gonzales told Mueller he needed to know whether Mueller would resign if the President decided (b)(1), (b)(3) Mueller responded that he would have to take time to consider his actions, but that he "would have to give it serious consideration if the President decided to go ahead in the face of DOJ's finding." ~~(TS//STLW//SI//OC/NF)~~

Later that afternoon on March 16, Card called Comey to the White House for a meeting. According to Philbin's notes, "the back channel word from Judge Gonzales" was that President Bush might be willing to (b)(1), (b)(3) Prior to the meeting, Comey, Goldsmith, and Philbin agreed that Comey should be ready to convey to the White House that the Department would support (b)(1), (b)(3) ~~(TS//STLW//SI//OC/NF)~~

Philbin's notes indicate that at the meeting Card told Comey that the President was "wrestling" with the issue of whether to [redacted] (b)(1), (b)(3) and would decide "very soon." Card also expressed to Comey his displeasure that Comey had put in writing the Department's position on the legality of the program. ~~(TS//STLW//SI//OC/NF)~~

That evening, while attending a farewell dinner for a Department colleague at a local restaurant, Philbin received a call from David Addington indicating that he wanted to deliver a letter Gonzales had written to Comey. Philbin met Addington at the Department at 8:30 p.m. that night to accept the letter. Philbin's notes also indicate that Gonzales had called Comey in advance to tell Comey "not to get too overheated by the letter." (U)

Comey told us he recalled that Gonzales told him in the call that the White House would agree to work with the Department to fix the program and that Comey should not "overreact" to Gonzales's letter. Comey said he believed Addington, and not Gonzales, had actually drafted the letter, and that Gonzales sent it only to counter Comey's memorandum and to make a record on behalf of the White House. (U)

Gonzales's letter stated that the President had directed him to respond to Comey's memorandum. The letter stated:

> Your memorandum appears to have been based on a misunderstanding of the President's expectations regarding the conduct of the Department of Justice. While the President was, and remains, interested in any thoughts the Department of Justice may have on alternative ways to achieve effectively the goals of the activities authorized by the Presidential Authorization of March 11, 2004, the President has addressed definitively for the Executive Branch in the Presidential Authorization the interpretation of the law.[192]

The letter also excerpted the language of paragraph 10 from the March 11, 2004, Authorization, which recited the bases on which the President acted to reauthorize the program, and then concluded: "Please ensure that the

---

[192] Gonzales's letter also addressed Comey's comments about congressional notification. Citing *Department of the Navy v. Egan*, 484 U.S. 518 (1988) and a 2003 OLC opinion, Gonzales's letter stated that the President has the constitutional authority to define and control access to the nation's secrets, "including authority to determine the extent to which disclosure may be made outside the Executive Branch." ~~(TS//STLW//SI//OC/NF)~~

Department of Justice complies with the direction given in the Presidential Authorization."[193] ~~(TS//STLW//SI//OC/NF)~~

C. White House Agrees to [redacted] (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~

Notwithstanding Gonzales's letter, on March 17, 2004, the President decided to [redacted] (b)(1), (b)(3) effective at midnight on March 26, 2004. According to Mueller's program log, Gonzales called Comey to advise him of the President's decision on March 17, 2004, and Comey passed this information to Mueller later that day. Comey, in an e-mail dated March 17, expressed relief at the President's decision, writing:

> Today, in a remarkable development, we stepped back from the brink of disaster. All seems well in the Government. The right thing was done. ~~(TS//STLW//SI//OC/NF)~~

Gonzales told the OIG during his interview that he could not say whether the prospect of resignations at the Department and the FBI may have had an impact on the President's decision.[194] We were not able to interview others at the White House to determine what specifically caused the program to be modified in accord with the Department's legal position. (U)

The President's directive was expressed in two modifications to the March 11, 2004, Presidential Authorization. These modifications, as well as the operational and legal implications of the President's decision for the Department and the FBI, are described in the next sections. ~~(TS//SI//NF)~~

1. March 19, 2004, Modification (U)

On March 19, 2004, the President signed, and Gonzales certified as to form and legality, a Modification of the March 11, 2004, Presidential

---

[193] Comey stated that he did not believe Gonzales wrote this letter. He stated that "Addington was the flame-thrower" and that Gonzales was generally more reasonable and moderate. Comey said that Gonzales had later apologized to both Comey and Ashcroft for his conduct during the March 10 incident at the hospital and had even come around to agree with Philbin and Goldsmith's analysis regarding the program. Gonzales told the OIG that he did not apologize to Ashcroft for the incident in the hospital because he had been instructed by the President to go there, but stated that he "regretted" the incident. (U)

[194] However, when Gonzales commented on a draft of this report, he told the OIG that the prospect of resignations at the Department and the FBI were not the reason for the President's decision. Gonzales stated that he could not elaborate on this statement due to executive privilege considerations. (U)

Authorization. The first paragraph of the Modification stated that "this memorandum, as a policy matter, modifies the Presidential Authorization of March 11, 2004 as set forth below . . . and (b)(1), (b)(3) granted by all the Presidential Authorizations to the extent set forth [in the Modification]." The March 19 Modification made two significant changes to the existing Authorization and a third important change affecting all Authorizations. To allow for a (b)(1), (b)(3) these changes were to become effective beginning at midnight on March 26, 2004. ~~(TS//STLW//SI//OC/NF)~~

First, the March 19 Modification inserted language to narrow content collection (basket 1) to al Qaeda and affiliated terrorist groups, as the Department had advised. The new content collection authority in paragraph 4(a) of the March 11 Authorization, with the new language from the March 19 Modification indicated in italics, was:

> acquire a communication (including but not limited to a wire communication carried into or out of the United States by cable) for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe such communication originated or terminated outside the United States and a party to such communication is a group engaged in international terrorism, or activities in preparation therefor, or any agent of such a group, *provided that such group is al Qa'ida, is a group affiliated with al Qa'ida, or is another group that I determine for purposes of this Presidential Authorization is in armed conflict with the United States and poses a threat of hostile action within the United States*[.] ~~(TS//STLW//SI//OC/NF)~~

Modification, March 19, 2004, para. 2(a)(italics and brackets added). This additional language resulted in (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~

Second, the Modification (b)(1), (b)(3) The language, with the deleted language in brackets and the insertion indicated in italics, was:

(b)(1), (b)(3)

(b)(1), (b)(3)

Modification, March 19, 2004

(b)(1), (b)(3)

Third, the March 19 Modification

(b)(1), (b)(3)

Modification, March 19, 2004

(b)(1), (b)(3)

Each Presidential Authorization had contained a directive to the Secretary of Defense not to disclose the program outside the Executive Branch without the President's approval. The Modification reiterated that any change was not intended to reverse the President's control over access to the program. ~~(TS//STLW//SI//OC/NF)~~

(b)(1), (b)(3)

---

[105] The ultimate disposition of this previously obtained (b)(1), (b)(3) was subsequently addressed in an April 2, 2004, Modification, and thereafter in an August 2004 Presidential memorandum to the Secretary of Defense, as described below in subsection 6. ~~(TS//STLW//SI//OC/NF)~~

(b)(5) [redacted] 196 The President's decision to [redacted] (b)(5) (b)(1) (b)(3)

~~(TS//STLW//SI//OC/NF)~~

(b)(1) (b)(3) [redacted]

b1, b3, b7E

196 Bradbury was nominated to be Assistant Attorney General for OLC in June 2005. He was not confirmed for this position, and told us that after exhausting the time period for use of the "Acting" title under the Vacancies Reform Act of 1998 (see 5 U.S.C. § 3345 et seq.) in April 2007, he reverted to Principal Deputy Assistant Attorney General, the position he had held prior to his nomination. As head of OLC, Bradbury became responsible for briefing members of Congress on OLC's legal analyses concerning the program as well as on the Presidential Authorizations. Bradbury's access to these documents and the officials responsible for drafting them provided him significant background information on the changes to the program. (U)

197 [redacted]

b1, b3, b7E

(b)(1), (b)(3), (b)(5)

2. (b)(1), (b)(3) b1, b3, b7E

(b)(1), (b)(3), (b)(5) b1, b3, b7E

b1, b3, b7E

3. (b) (5), (b)(1), (b)(3)

(b)(1), (b)(3), (b) (5)

198

b1, b3, b7E

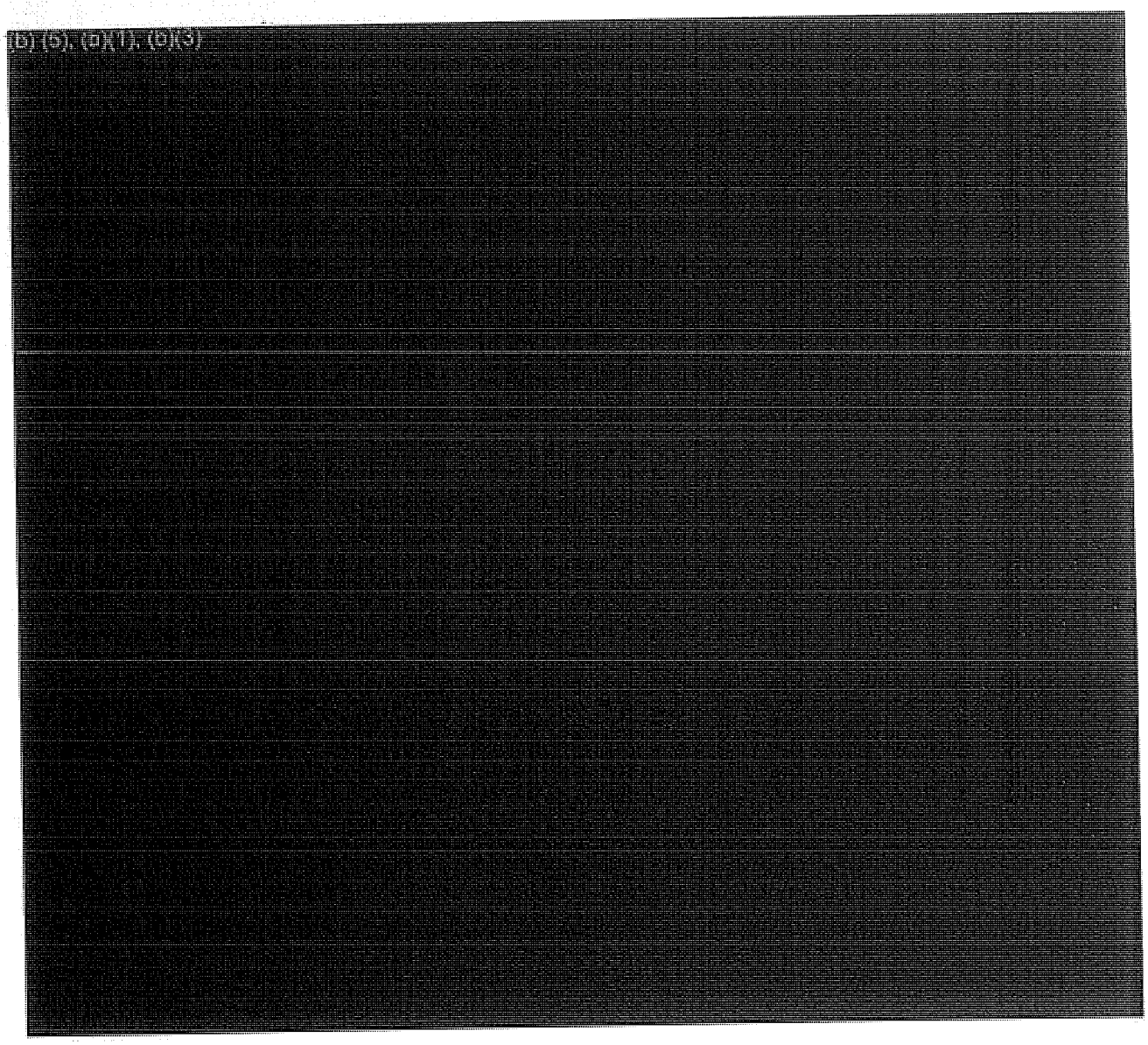
199

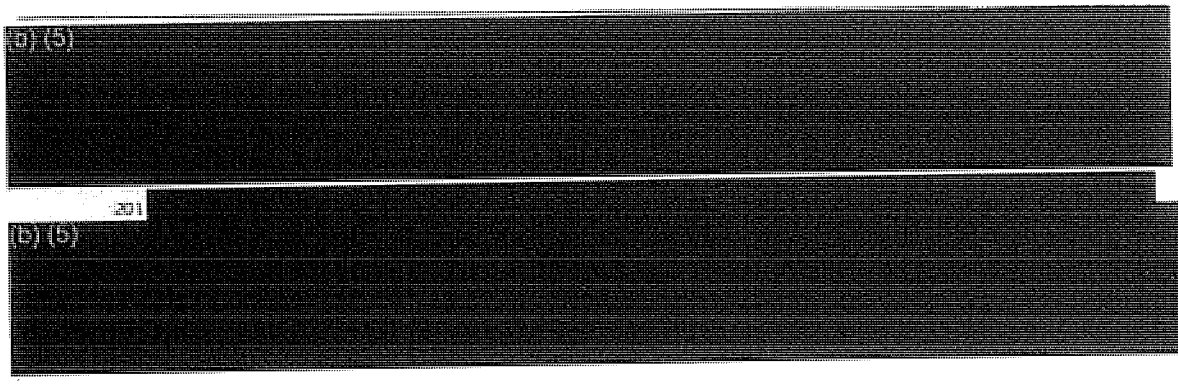
(b) (5), (b)(1), (b)(3)

200

(b) (5), (b)(1), (b)(3)

(Cont'd.)


(b) (5), (b)(1), (b)(3)


(b) (5)
(b) (5)

4. (b)(1), (b)(3)

(b)(1), (b)(3), (b)(5)

b1, b3, b7E

5. **Judge Kollar-Kotelly is Presented with the OLC Legal Analysis Regarding** (b)(1), (b)(3), (b)(5) (~~TS//STLW//SI//OC/NF~~)

As noted above, Judge Kollar-Kotelly was made aware on March 14, 2004, that the March 11 Authorization had been signed by the President

but had not been certified as to form and legality by the Justice Department. On March 18, 2004, Goldsmith, Philbin, Baker, and Gonzales met with Judge Kollar-Kotelly to further brief her on the status of the program. According to an internal OLC memorandum, they advised her that forthcoming legal opinions from OLC would allay her concerns about the use of program-derived information in FISA applications.[202] ~~(TS//STLW//SI//OC/NF)~~

The OIG reviewed a handwritten letter from Judge Kollar-Kotelly to OIPR Counsel Baker, which appeared to have been written just after the initiation of (b)(1), (b)(3) mandated in the March 19, 2004, Modification. Baker told us that the handwritten letter should be viewed as an informal draft designed to convey Judge Kollar-Kotelly's preliminary understanding of the issues raised by the changes to the Stellar Wind program. In the letter, Judge Kollar-Kotelly reiterated her position that Stellar Wind-derived information should be excluded from FISA applications, writing, "so there is no misunderstanding, I will not sign a FISA application which contains any information derived from and/or obtained from the [Stellar Wind] program," including applications in which a Stellar Wind tip "was the sole or principal factor in starting an investigation by any of the agencies, even if the investigation was conducted independently of the tip from [Stellar Wind]." Judge Kollar-Kotelly also requested, as a precondition to her agreeing to sign FISA applications in the future, that OIPR clarify in writing its proposal for reviewing FISA applications to ensure that all Stellar Wind-derived information had been excluded. Baker told us that he had a lot of "verbal back and forth" with Judge Kollar-Kotelly to explain OIPR's scrubbing procedures. ~~(TS//STLW//SI//OC/NF)~~

In late March 2004, OLC provided Judge Kollar-Kotelly with a draft analysis discussing [redacted]

(b)(1), (b)(3), (b)(5)

[redacted]

---

202 As described below, these legal opinions, which addressed the legality of [redacted] (b)(1), (b)(3) were provided to Judge Kollar-Kotelly in late March and early April 2004. ~~(TS//STLW//SI//OC/NF)~~

203 Chapter Three, Section II B contains a description of this process. (U)

[redacted]

On March 26, 2004, OLC completed a draft memorandum for Baker entitled "Use or Disclosure of Certain Stellar Wind Information in Applications Under FISA." This memorandum addressed the inclusion in FISA applications of information derived indirectly from (b)(1), (b)(3), (b)(5) .[205] OLC also provided Judge Kollar-Kotelly with a copy of its draft legal analysis.[206] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

---

[204] This argument is discussed below in connection with Goldsmith's May 6, 2004, legal analysis. (U)

[205] With respect to (b)(1), (b)(3), (b)(5) the memorandum stated that the Department did not believe the acquisition of such information was subject to any constitutional restraints or statutory restrictions, but that "[t]o the extent Judge Kollar-Kotelly has concerns about those conclusions, we note that the analysis in this memorandum independently demonstrates that there are no legal restrictions on the use of information indirectly derived from (b)(1), (b)(3), (b)(5) tippers in FISA applications." ~~(TS//STLW//SI//OC/NF)~~

[206] The draft memorandum did not address inclusion in FISA applications of information derived *directly* from the program because OIPR had successfully managed to address Judge Kollar-Kotelly's order to exclude such information. ~~(TS//STLW//SI//OC/NF)~~

6. April 2, 2004, Modification (U)

Attorney General Ashcroft's doctors cleared him to resume his duties as Attorney General as of March 31. Comey advised Ayres in a March 30, 2004, memorandum that as of 7:00 a.m. on March 31, the Attorney General was no longer "absent or disabled" within the meaning of 28 U.S.C. § 508(a), and that as of that time Comey could no longer exercise the duties of the Office of Attorney General pursuant to the statute. A copy of the memorandum was sent to White House Counsel Gonzales and other senior Department officials. (U)

On April 2, 2004, President Bush signed, and Gonzales certified as to form and legality, a second Modification of the March 11, 2004, Presidential Authorization. This modification addressed only (b)(1), (b)(3) activities of the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

(b)(1), (b)(3)

Thus, under this new standard (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~

(b)(1), (b)(3)

(b)(1), (b)(3), (b) (5)

[redacted]

[redacted] An April 5, 2004 Goldsmith memorandum to file stated that OLC worked with Addington to craft the new (b)(1), (b)(3), (b) (5) standard. ~~(TS//STLW//SI//OC/NF)~~

[redacted] Bradbury distinguished the limitation on (b)(1), (b)(3), (b) (5) ~~(TS//STLW//SI//OC/NF)~~

(b)(1), (b)(3)
~~(TS//STLW//SI//OC/NF)~~

7. (b)(1), (b)(3) Standard is Conveyed to the FBI ~~(TS//SI//NF)~~

The OIG sought to determine how the presidentially authorized limitations on (b)(1), (b)(3) in the Modifications and subsequent Authorizations were communicated to FBI employees responsible for tipping Stellar Wind information to the field. ~~(TS//STLW//SI//OC/NF)~~

A former Unit Chief in the Communications Analysis Unit (CAU) within the FBI's Communications Exploitation Section (CXS) of the Counterterrorism Division told us he became aware that at some point the scope of collection under Stellar Wind was narrowed to include only (b)(1), (b)(3) He said this information was passed along to him and others at the FBI during either a monthly or quarterly meeting with NSA representatives. He said the (b)(1), (b)(3) practice was "taken very seriously" by the NSA. As an example, he said that Requests for Information (RFI) from the FBI to the NSA on numbers not associated with (b)(1), (b)(3) were rejected by the NSA as outside the scope of the revised Authorization. ~~(TS//STLW//SI//OC/NF)~~

An FBI Supervisory Special Agent in the CAU's unit co-located at the NSA (called Team 10), told us that when he first began collection and analysis work under the program, (b)(1), (b)(3) were "fair game." He recalled that at some later point the scope of collection (b)(1), (b)(3) He said that (b)(1), (b)(3) was rigorously adhered to and was "scrutinized very closely." He said that when the FBI requested that the NSA collect information on a particular number, the NSA closely analyzed the number and requested supporting information from the FBI before querying the Stellar Wind database. This supervisor also stated that the NSA did a good job of keeping the co-located FBI personnel informed of changes to the scope of collections. He said this information typically would be conveyed to appropriate personnel during the daily "all hands meetings." ~~(TS//STLW//SI//OC/NF)~~

8. Office of Legal Counsel Assesses NSA's Compliance with New Collection Standards ~~(TS//SI//NF)~~

Goldsmith told us that during the week of March 29, 2004, he and Philbin conducted an "audit" of the Stellar Wind program to ensure that the querying of (b)(1), (b)(3) was being conducted in accordance with the Presidential Authorizations. ~~(TS//STLW//SI//OC/NF)~~

Goldsmith said that while resources were not available to conduct a "professional" audit, he visited the NSA and reviewed with relevant NSA officials the legal parameters for querying [redacted] which as discussed above required a showing of reasonable articulable suspicion that the target belonged to a group that was engaged in international terrorism.[209] Goldsmith told the OIG that as part of the review, he and Philbin familiarized the NSA with the new collection parameters [redacted] ~~(TS//STLW//SI//OC/NF)~~

To conduct their review, Goldsmith and Philbin requested that the NSA [redacted] ~~(TS//STLW//SI//OC/NF)~~

On April 15, 2004, Goldsmith reported the results of his and Philbin's review to [redacted] the Assistant General Counsel for Operations in the NSA's Office of General Counsel. On April 22, 2004, Goldsmith memorialized his conversation with [redacted] in a memorandum to file. In the memorandum, Goldsmith noted four types of problems he and Philbin found in their review. [redacted] The memorandum stated that Goldsmith also conveyed this advice to Vito Potenza, the NSA's Acting General Counsel at the time. ~~(TS//STLW//SI//OC/NF)~~

9. May 5, 2004, Presidential Authorization ~~(TS//SI//NF)~~

As noted above, the March 11, 2004, Presidential Authorization, as modified, was set to expire on May 6, 2004. On May 5, the President signed another Authorization extending the Stellar Wind program through June 24, 2004. Unlike the March 11 Authorization and the two modifications that

[209] [redacted]

followed it, the May 5 Authorization was certified as to form and legality by Attorney General Ashcroft. ~~(TS//SI//NF)~~

The May 5, Authorization contained the language from the March 11 Authorization narrowing the scope of (b)(1), (b)(3) The May 5 Authorization also included the paragraph defining the scope of (b)(1), (b)(3) as modified on March 19 to encompass only (b)(1), (b)(3) the May 5 Authorization reiterated the new collection standard set forth in the April 2, 2004, Modification, which required that (b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~

With minor variations, the collection standards and other language set forth in the May 5, 2004, Presidential Authorization remained unchanged in all of the subsequent Authorizations.[211] ~~(TS//STLW//SI//OC/NF)~~

10. May 6, 2004, OLC Memorandum ~~(TS//SI//NF)~~

On May 6, 2004, Goldsmith completed a revised OLC memorandum on the legality of the Stellar Wind program. The 108-page document stated that it was written for the Attorney General in response to his request for OLC "to undertake a thorough reexamination of the Stellar Wind program as it is currently operated to confirm that the actions that the President has directed the Department of Defense to undertake through the National Security Agency (NSA) are lawful." ~~(TS//SI//NF)~~

The memorandum traced the history of the program and analyzed the legality of each of the three collection baskets in light of applicable statutes, Executive Orders, cases, and constitutional provisions. ~~(TS//STLW//SI//OC/NF)~~

---

[210] This Authorization also dropped the language describing the legal bases on which the President relied in ordering the continuation of the program in the March 11, 2004, Authorization. ~~(TS//SI//NF)~~

(b)(1), (b)(3), (b) (5)

The memorandum noted that Section 111 of FISA, 50 U.S.C. § 1811, providing that the President "may authorize electronic surveillance without a court order . . . to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by Congress," made it clear that FISA expressly addresses electronic surveillance during wartime.[212] The memorandum stated that the Authorization for Use of Military Force (AUMF) passed by Congress shortly after the attacks of September 11, 2001, gave the President authority to use both domestically and abroad "all necessary and appropriate force," including signals intelligence capabilities, to prevent future acts of international terrorism against the United States. According to the memorandum, the AUMF was properly read as an express authorization to conduct targeted electronic surveillance against al Qaeda and its affiliates, the entities responsible for attacking the United States. ~~(TS//STLW//SI//OC/NF)~~

The memorandum noted that the legislative history of FISA indicates that the 15-day window was "thought sufficient for the President to secure legislation easing the restrictions of FISA for the conflict at hand." Quoting H.R. Conf. Rep. No. 95-1720, at 34, reprinted in U.S.C.C.A.N. 4048, 4063 ("[T]he conferees intend that this period will allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency"). According to the OLC memorandum, "The Congressional Authorization functions as precisely such legislation: it is emergency legislation passed to address a specific armed conflict and expressly designed to authorize whatever military actions the Executive deems appropriate to safeguard the United States." ~~(TS//SI//NF)~~

The memorandum concluded that at a minimum the AUMF made the application of FISA in a wartime context sufficiently ambiguous that the doctrine of constitutional avoidance properly applied to avoid a conflict between FISA and the presidentially authorized Stellar Wind program. Alternatively, the memorandum argued that FISA, as applied in the particular circumstances of a President directing surveillance of the enemy to prevent future attacks upon the nation, represented an unconstitutional infringement on the President's Article II Commander-in-Chief powers. ~~(TS//STLW//SI//OC/NF)~~

These two arguments also were cited in support of [redacted] (b) (5), (b)(1), (b)(3)

[212] As discussed in section I of this chapter, the legal implications of this provision of FISA was not addressed in the memoranda John Yoo had drafted in support of the program in late 2001. ~~(TS//SI//NF)~~

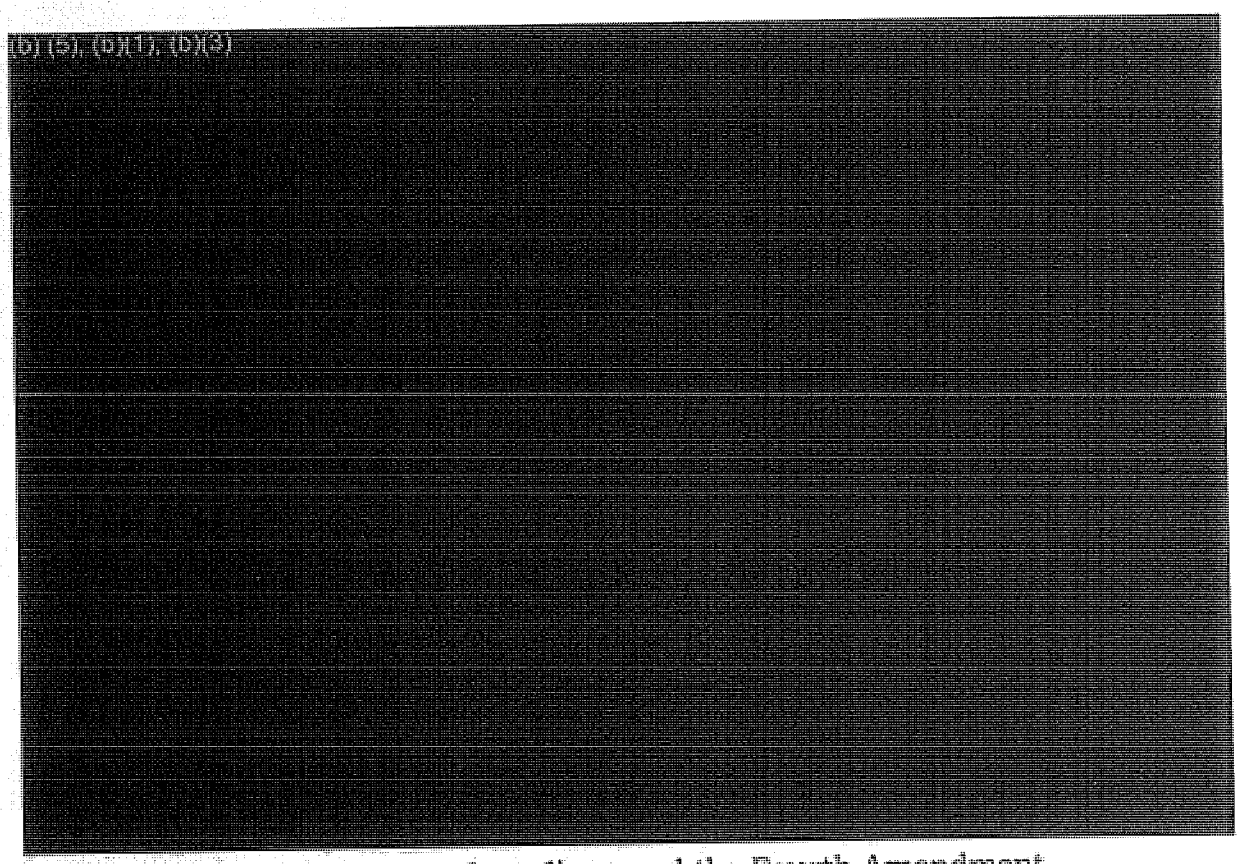
(b)(1), (b)(3), (b) (5)

The memorandum also analyzed the legal rationale for
(b)(1), (b)(3), (b) (5)
(~~TS//STLW//SI//OC/NF~~)

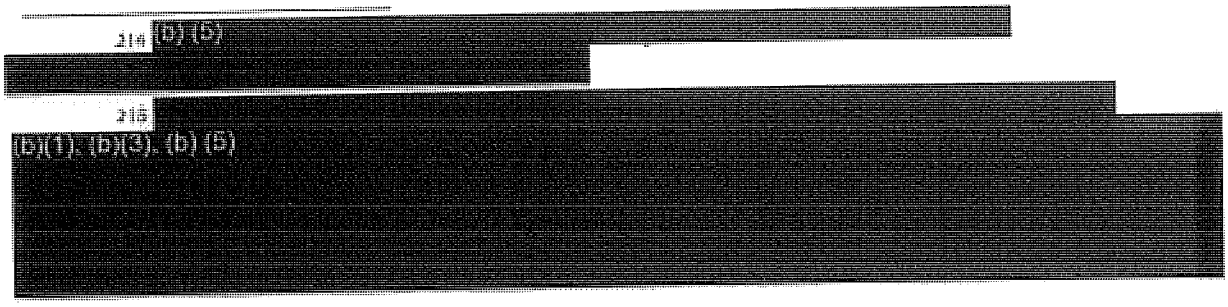
(b) (5), (b)(1), (b)(3)

[redacted]

(b) (5), (b)(1), (b)(3)



Finally, the memorandum discussed the Fourth Amendment implications of the Stellar Wind program. To determine whether interception of (b)(1), (b)(3), (b) (5) violated the Fourth Amendment's prohibition against unreasonable searches, the memorandum analyzed whether the importance of the government's interest in this collection outweighed the individual privacy interests at stake. Citing various authorities, including Supreme Court opinions, the Federalist Papers, (b)(1), (b)(3) and congressional testimony, the memorandum concluded that "the government's overwhelming interest in detecting and thwarting further al Qaeda attacks is easily sufficient to make reasonable the intrusion into privacy involved in intercepting selected communications." The memorandum noted that the weight of the



government's interest in this regard could change over time if the threat from al Qaeda were deemed to recede. ~~(TS//STLW//SI//OC/NF)~~

The memorandum also analyzed telephone and e-mail meta data collection under the Fourth Amendment. The memorandum concluded, based on the Supreme Court's holding in *Smith v. Maryland*, 442 U.S. 735, 742 (1979), that there is no legitimate expectation of privacy in the numbers dialed to place telephone calls. Referring to cases holding that no expectation of privacy attached to the address information on either letter mail or e-mail, the memorandum concluded that no Fourth Amendment privacy interests were implicated in the collection of e-mail meta data. ~~(TS//STLW//SI//OC/NF)~~

In sum, the May 6 memorandum was the most comprehensive assessment of the Stellar Wind program drafted by the Office of Legal Counsel. [redacted] (TS//STLW//SI//OC/NF)

[redacted] (TS//STLW//SI//OC/NF)

[redacted] (TS//STLW//SI//OC/NF)

~~(TS//STLW//SI//OC/NF)~~

III. OIG Analysis (U)

A. Department's Access to and Legal Review of Stellar Wind Program Through May 2004 ~~(TS//SI//NF)~~

The Justice Department's access to the Stellar Wind program was controlled by the White House, and Gonzales told the OIG that the President decided whether non-operational personnel, including Department lawyers, could be read into the program. Department and FBI officials told us that obtaining approval to read in Department officials and FISA Court judges involved justifying the requests to Addington and Gonzales, who effectively acted as gatekeepers to the read-in process for non-operational officials. In contrast, according to the NSA, operational personnel at the NSA, CIA, and the FBI were read into the program on the authority of the NSA Director, who at some point delegated this authority to the Stellar Wind Program Manager. ~~(TS//SI//NF)~~

Various officials we interviewed about the issue uniformly agreed that the White House sought to strictly limit overall access to the Stellar Wind program. We believe that this policy was applied at the Department in an unnecessarily restrictive manner prior to March 2004, and was detrimental to the Department's role in the operation of the program through that period. We also believe that Attorney General Ashcroft, as head of the Department, was responsible for seeking to ensure that the Department had adequate attorney resources to conduct a thorough and accurate review of the legality of the program. Because Ashcroft did not agree to be interviewed for this investigation, we were unable to determine the extent of his efforts to press the White House to read in additional Department officials between the program's inception in October 2001 and the critical events of March 2004. ~~(TS//SI//NF)~~

In Chapter Three we described how the Department's early involvement in the Stellar Wind program was limited to the participation of only three attorneys – Attorney General Ashcroft, OLC Deputy Assistant Attorney General John Yoo, and Counsel for Intelligence Policy James Baker.[216] Working alone, Yoo drafted several legal memoranda in 2001 and 2002 advising the Attorney General and the White House that the program was legally supported. In reliance on Yoo's advice, Attorney General Ashcroft certified the legality of the Presidential Authorizations to implement the program. ~~(TS//SI//NF)~~

Because Yoo worked alone, his legal analysis was not reviewed by other attorneys, either in OLC or elsewhere in the Department.[217] Even

---

216 Counsel for Intelligence Policy James Baker was read into the program in either late 2001 or January 2002. But Baker appears to have been read in only because he inadvertently came across information that suggested such a program existed. While Baker had involvement in several aspects of the program, he had no involvement in drafting or reviewing Yoo's legal memoranda supporting the program. Daniel Levin, who served as both Chief of Staff to FBI Director Mueller and briefly as a national security counselor to Ashcroft, also was read into Stellar Wind at the inception of the program. However, Levin only served for two months at the Department during this early phase of Stellar Wind and had very limited involvement in the program during this period. Levin told us he was read into Stellar Wind along with Director Mueller at the FBI and that he understood that he was being cleared into the program as an FBI official. We therefore consider Levin to be an FBI read-in, not a Department read-in. ~~(TS//STLW//SI//OC/NF)~~

217 Gonzales told us that he thought Yoo may have assigned discrete tasks to other attorneys in connection with his work on the Stellar Wind legal memoranda. Because Yoo declined our request for an interview, we were unable to confirm this. In any event, no other attorneys were read into Stellar Wind and therefore would not have been permitted to work on or review those portions of the memoranda that contained Top Secret/Sensitive Compartmented Information (TS/SCI) related to the Stellar Wind program. By contrast, Yoo had at least one other OLC attorney to assist him in drafting other OLC legal memoranda on the detainee interrogation program during the 2001 to 2003 period, and these memoranda were reviewed by another OLC Deputy Assistant Attorney General

(Cont'd.)

when Jay Bybee became the OLC Assistant Attorney General in November 2001, and was therefore Yoo's supervisor, Bybee was not read into the program.[218] Bybee told us he also was unaware that Yoo was providing advice to the Attorney General and the White House on the legal basis to support the program. ~~(TS//SI//NF)~~

We believe that even before Patrick Philbin voiced his initial concerns with Yoo's analysis in 2003, the circumstances in 2001 and 2002 plainly called for additional Department resources to be applied to the legal review of the program and that it was the Attorney General's responsibility to be aware of this need and to take steps to address it. Moreover, because Ashcroft met frequently with the President on national security matters, he would have been well-positioned to request additional legal resources if he believed they were necessary. ~~(TS//SI//NF)~~

The facts suggest that Ashcroft had some awareness and concern that Yoo was working on the legal justification for the Stellar Wind program without any Department assistance or oversight, and possibly was advising the White House directly of his findings. Based on accounts of the incident in Ashcroft's hospital room in March 2004, Ashcroft made specific complaints to Gonzales and Card about insufficient legal resources at the Department and that the Department had been "cut out of the whole affair." He had also expressed frustration to Comey months earlier about being "in a box" with Yoo. Further, according to Goldsmith, when Goldsmith first interviewed for the position of Assistant Attorney General for OLC in 2003, Ashcroft and his Chief of Staff alluded to concerns over being kept informed of matters the Office of Legal Counsel was working on and the importance of keeping the Attorney General "in the loop." We also note that Yoo's November 2, 2001, memorandum to Ashcroft indicated that "[b]ecause of the highly sensitive nature of this subject and the time pressures involved, this memorandum has not undergone the usual editing and review process for opinions that issue from our Office [OLC]." ~~(TS//SI//NF)~~

While we believe that Ashcroft may have been aware that Yoo was working alone on the Stellar Wind analysis and had concerns about this, we do not know whether or how hard he pressed the White House to read in additional attorneys to assist or supervise Yoo. At the same time, however,

---

(Philbin) and approved by the OLC Assistant Attorney General (Bybee). The detainee interrogation program also was classified as TS/SCI. We also note that Philbin's background in telecommunications law would have made him a logical choice to assist Yoo on the Stellar Wind legal analysis. ~~(TS//SI//NF)~~

[218] In contrast, Bybee was allowed to supervise Yoo's work drafting legal memoranda concerning a detainee interrogation program during the same time period. ~~(TS//SI//NF)~~

we cannot assume that any requests by Ashcroft for additional attorney read-ins would have been granted by the White House. Gonzales told us that Ashcroft had requested that Deputy Attorney General Larry Thompson and Ashcroft's Chief of Staff David Ayres be read in. However, neither request was approved.[219] Gonzales stated that he did not recall Ashcroft requesting additional read-ins beyond Thompson and Ayres. (U)

In analyzing the read-in situation at the Department during Yoo's tenure, we also considered that Ashcroft certified the program as to its legality each time the program came up for renewal, and did so at a time when Yoo's legal advice was the only Department guidance available concerning the program's legality. We believe the fact that only three Department attorneys were read into Stellar Wind through mid-2003 may have been due at least in part to Ashcroft's routine recertifications of the Presidential Authorizations during this period. As noted in Chapter Three, Gonzales told us that it was up to the Attorney General to decide how to satisfy his legal obligations as Attorney General, and that if Ashcroft believed more attorneys were needed for this purpose, he could have asked the President to approve additional Department read-ins. Gonzales also told us that Ashcroft's continued certifications of the Presidential Authorizations supported Gonzales's belief that Ashcroft was satisfied with the quality of the legal advice he was receiving at the time within the Department. ~~(TS//SI//NF)~~

There is evidence as well that Gonzales, as White House Counsel, was satisfied with Yoo's legal memoranda supporting the program. Gonzales told us that although he did not believe Yoo's first two memoranda fully addressed the White House's understanding of the Stellar Wind program, Gonzales believed that they described as lawful activities that were broader than those carried out under Stellar Wind, and that Yoo's memoranda therefore "covered" the program.[220] ~~(TS//SI//NF)~~

---

[219] Deputy Attorney General Thompson resigned from the Department in August 2003, so Ashcroft's request to have him read into the program would have been made before that time. That neither Thompson nor Ayres was read in contrasts with the decision to allow in the case of [redacted] to be briefed about the program in 2002, and [redacted] to be read into the program in 2003. The OIG does not know who authorized these read-ins. ~~(TS//SI//NF)~~

[220] We were troubled by Gonzales's suggestion that Yoo's memoranda covered the program because the memoranda determined to be lawful a range of "hypothetical" activities that were interpreted by Gonzales to be broader than those actually carried out under Stellar Wind. Such an approach, if deemed acceptable by the "client" (in this case the White House), would encourage the Office of Legal Counsel to draft broad and imprecise (Cont'd.)

However, even apart from the limited number of Department read-ins, we believe that the White House imposed excessively strict controls over access to the program in other ways that were detrimental to the Department's ability to provide the White House with the soundest possible legal advice. For instance, we found no indication that Yoo coordinated his legal analysis with the NSA. According to Michael Hayden, the Director of the NSA when Stellar Wind began, the NSA relied on its Office of General Counsel, and not the Department of Justice, for advice as to the legality of the program when it was created. However, we found that the NSA's Office of General Counsel did not coordinate its legal advice with the Department, and even as late as 2003 the NSA General Counsel was prevented by the White House from reviewing the Department's legal opinions on the program.[221] Hayden also told the OIG that he was "surprised with a small 's'" that the Department did not participate in the early meetings with him and White House officials when Stellar Wind was first conceived. In addition, Addington instructed Philbin not to discuss the program with Baker, who as Counsel for Intelligence Policy was responsible for representing the government before the FISA Court.[222] ~~(TS//SI//NF)~~

We believe that that White House should have allowed and even encouraged coordination between the Department and the NSA regarding the development of the legal analysis of the program, especially as this analysis was first being formulated in late 2001. Such interaction between the Department and other Executive agencies is a mainstay of traditional OLC practice, and we believe its absence here contributed to factual errors in Yoo's opinions regarding the operation of the program. ~~(TS//SI//NF)~~

Although we could not determine exactly why Yoo remained the only Department attorney assigned to assess the program's legality from 2001 until his departure in May 2003, we discuss below our belief that this practice represented an extraordinary and inappropriate departure from OLC's traditional review and oversight procedures and resulted in significant harm to the Department's role in the program. ~~(TS//SI//NF)~~

When Yoo left the Department in May 2003, he was replaced by Patrick Philbin, who was read into the program to advise Ashcroft whether he could continue to certify the Presidential Authorizations as to their form

---

legal analysis and would discourage the type of careful scholarship to which the OLC traditionally aspires. ~~(TS//SI//NF)~~

[221] In addition, the NSA Office of the Inspector General, which wanted to conduct an internal audit of the program during this period, was prevented by Addington from reviewing the Justice Department's legal memoranda supporting the program. (U//~~FOUO~~)

[222] Philbin told the OIG that he spoke with Baker about the program despite Addington's instruction not to. (U)

and legality. When Goldsmith became the OLC Assistant Attorney General in October 2003, Philbin pressed Addington to have Goldsmith read in, and Goldsmith became the first head of OLC to be read into the program. As noted, Goldsmith's predecessor Jay Bybee was never read into the program. ~~(TS//SI//NF)~~

Thus, by the end of 2003, a total of only 5 Department officials – Yoo, Ashcroft, Baker, Philbin, and Goldsmith – had been read into Stellar Wind. By comparison, and as shown in Chart 4.1 below, we determined that many other individuals throughout the government were read into the program. Through the same period, [redacted]

~~(TS//STLW//SI//OC/NF)~~

[redacted]

The assignment of only one Department attorney, John Yoo, to conduct a legal review of the program without assistance or oversight from anyone else at the Department, combined with the White House's decision to prevent the NSA from reviewing Yoo's work, resulted in legal opinions by Yoo that were later determined by OLC to be so inaccurate and incomplete

---

223 This table was derived from NSA read-in information. Justice Department read-ins include [redacted] OIG personnel who were read into Stellar Wind in 2006. (U//~~FOUO~~)

as to be regarded as not covering key aspects of the Stellar Wind program. Given the enormously complex nature of the program from both a technical and legal perspective, coupled with the fact that he was working alone, it was not altogether surprising that Yoo's analysis contained inaccuracies and omitted critical elements, particularly given the pressure to generate a legal analysis within weeks of the program's implementation. However, Yoo's analysis did not change or include a more accurate description of the program's operation over the course of his 20-month tenure with the OLC. ~~(TS//SI//NF)~~

After reviewing Yoo's legal opinions on the program, Goldsmith and Philbin quickly discovered what they characterized as serious flaws in Yoo's legal analysis. These flaws included Yoo's failure to describe [redacted] being conducted by the NSA under the Stellar Wind program and his failure to assess the legality of this and other activities as they were carried out by the NSA. ~~(TS//STLW//SI//OC/NF)~~

Specifically, both Goldsmith and Philbin stated that Yoo mischaracterized in his memoranda the nature and scope of the NSA's [redacted] They stated that Yoo's characterization of this activity in his 2001 and 2002 legal memoranda was factually flawed and that Yoo appears to have based his legal analysis of this aspect of the program on an incomplete and inaccurate description both of [redacted] and the [redacted][224] Both Goldsmith and Philbin also acknowledged that they initially incorrectly believed the NSA's [redacted] was broader than it in fact was under the program. However, unlike Yoo, Goldsmith and Philbin accurately

[redacted]

[224] [redacted]

characterized the collection [redacted] and thus their legal advice was based on facts that more closely reflected the actual operation of the program.[225] ~~(TS//STLW//SI//OC/NF)~~

In addition, Goldsmith and Philbin discovered that Yoo's assertion that the President had broad authority to conduct electronic surveillance without a warrant pursuant to his Commander-in-Chief powers under Article II of the Constitution, particularly during wartime, never addressed the FISA provision that expressly addressed electronic surveillance following a formal declaration of war. See 50 U.S.C. § 1811. Goldsmith also criticized Yoo's legal memoranda for failing to support Yoo's aggressive Article II Commander-in-Chief theory with a fully developed separation of powers analysis, and instead offering only sweeping conclusions. As an example, Goldsmith cited Yoo's assertion that reading FISA to be the "exclusive statutory means for conducting electronic surveillance for foreign intelligence" amounts to an "unconstitutional infringement on the President's Article II authorities."[226] Moreover, noted Goldsmith, Yoo omitted from his separation-of-powers discussion any analysis of how the Youngstown Steel Seizure Case, a seminal Supreme Court decision on the distribution of governmental powers between the Executive and Legislative Branches during wartime, would affect the legality of the President's actions with respect to Stellar Wind.[227] ~~(TS//STLW//SI//OC/NF)~~

In reliance on Yoo's advice, the Attorney General certified the program "as to form and legality" some 20 times before Yoo's analysis was determined to be flawed by his successors in OLC and by attorneys in the Office of the Deputy Attorney General. We agree with many of the criticisms offered by Department officials regarding the practice of allowing a single Department attorney to develop the legal justification for the program

[redacted]

[redacted]

[redacted]

during its early stage of operation. We summarize these criticisms below. ~~(TS//SI//NF)~~

Goldsmith described as "crazy" and "outrageous" the assignment of an OLC Deputy Assistant Attorney General to provide legal advice to the White House without the knowledge or concurrence of the Senate-confirmed Assistant Attorney General for OLC, who is accountable for the legal positions taken by the office. (U)

Goldsmith said that not a single critical eye reviewed Yoo's work on a program that Goldsmith described as "flying in the face" of the conventional understanding of the law at the time. Goldsmith noted that Yoo's legal memoranda did not include facts about how the Stellar Wind program operated in practice, and he surmised that Yoo instead might have "keyed off" the Presidential Authorizations rather than NSA's actual collection practices in developing his analysis. Goldsmith also said it was "insane" that Yoo's memoranda were not shared with the NSA. Goldsmith said that had the NSA reviewed these memoranda Yoo's failure to accurately describe the nature and scope of the collection by the NSA and the resulting "mismatch" between the actual practice and the wording of the Presidential Authorizations might have been detected earlier. ~~(TS//SI//NF)~~

Similarly, Daniel Levin, who was one of the first FBI officials to be read into Stellar Wind and who would later become Acting Assistant Attorney General for OLC upon Goldsmith's departure in June 2004, criticized allowing a single attorney to be the sole voice of the OLC concerning a program such as Stellar Wind. Levin stated that OLC has a special role at the Department and within the government, especially with "highly secret programs where opinions may never see the light of day." Under such circumstances, according to Levin, it is very difficult not to say "yes" to the White House – OLC's client – in the face of national security threats. Levin stated that unlike situations where a court places limitations on the positions the government may take, there are no such limitations when OLC considers a position that will remain secret, and it is easier to be more aggressive and "cut some corners" under such circumstances. ~~(TS//STLW//SI//OC/NF)~~

Levin stated that Yoo's memoranda justifying the program suffered from too little circulation and a lack of alternative views. He said that the OLC memoranda produced under Goldsmith's tenure were better, not because the authors were "smarter" than Yoo, but because the authors benefited from multiple viewpoints and input. Levin also said that he never understood why the Stellar Wind program was deemed so sensitive at the operational level. Levin said he appreciated that the program was politically sensitive, but added that it was a "huge mistake" to keep the program so closely held within the Department. ~~(TS//STLW//SI//OC/NF)~~

We believe that Goldsmith's and Levin's comments concerning the secrecy of Stellar Wind are especially relevant to the need for legally and factually sound OLC analysis with respect to classified national security programs. Because programs like Stellar Wind are not subject to the usual external checks and balances on Executive authority, OLC's advisory role is particularly critical to the Executive's understanding of potential statutory and Constitutional constraints on its actions. ~~(TS//STLW//SI//OC/NF)~~

Deputy Attorney General Comey also criticized the decision to allow a single person to assess the legality of the program on behalf of the Department. Comey told us that Goldsmith had once aptly described the Yoo situation to him as "the perfect storm" in which the following factors converged: the terrorist attacks of September 11, 2001; a "brilliant guy" at the Department who was "an aggressive advocate for executive power"; and a White House "determined to restore executive power." Comey expressed a degree of sympathy for Yoo, noting the extraordinary situation into which Yoo had been placed. Comey also observed that the response to September 11 essentially placed the policy burden on lawyers, who were now looked to by others for guidance as to what counterterrorism activities fell within the bounds of the law. However, Comey said that he believed White House officials "got what they ordered" by asking Yoo for opinions and restricting the number of persons with access to the program or the opinions.[228] ~~(TS//SI//NF)~~

Attorney General Ashcroft declined to be interviewed in our review, and we were thus unable to determine what his views were on the assignment of Yoo alone to conduct the legal review of the program. However, as noted above, witness accounts of his statements concerning the Yoo situation leave little doubt that Ashcroft was plainly upset with the White House for putting him "in a box" with Yoo. According to Goldsmith and Philbin, Ashcroft was direct about his grievances when Gonzales and Card came to see him in the hospital on March 10, 2004, including complaining that Ashcroft's Chief of Staff and until recently the Deputy Attorney General had not been allowed to be read into the program, and that he found it "very troubling that [redacted] people in other agencies" had been read into the program. What remains unclear is whether Ashcroft came to the realization that the Department had been given an insufficient number of read-ins only after Philbin and Goldsmith presented him with their concerns about the quality of Yoo's legal analysis, or at some point before. ~~(TS//SI//NF)~~

---

[228] As noted in Chapter Three, Yoo had been given the national security portfolio when he first joined the OLC in July 2001, several months before the attacks of September 11, 2001, and the inception of Stellar Wind. (U//~~FOUO~~)

We sought to obtain Yoo's and the White House's perspective on his selection as the sole Justice Department attorney to be read into Stellar Wind to provide advice on the legality of the program. We were not able to interview Yoo, who declined our request, or Addington and Card, who did not respond to our requests. ~~(TS//SI//NF)~~

The OIG asked Gonzales about how the White House determined who in the Department could be read into the program, but on the advice of Special Counsel to the President, Gonzales limited his answer to his personal views and declined to discuss internal White House deliberations that may have factored into the read-in decisions. Gonzales stated that he believed it was necessary for national security reasons to limit the number of read-ins to those "who were absolutely essential." Gonzales also stated that there had to be sufficient operational personnel at the NSA, CIA, and FBI read in for the purpose of running the program, while reading in additional lawyers at the Department had comparatively less value because all lawyers will "have opinions" about the program. Yet, Gonzales also stressed to us that he welcomed the Department's reassessment of Yoo's opinions and encouraged Goldsmith and Philbin to re-examine the legal basis for the program in 2003 and 2004.[229] ~~(TS//SI//NF)~~

We think the proposition that the participation of Department attorneys to analyze the legality of a program as factually and legally complex as Stellar Wind should be limited for the reasons offered by Gonzales is shortsighted and counterproductive. First, it is evident that Stellar Wind was as legally complex as it was technically challenging. Just as a sufficient number of operational personnel were read into the program to assure its proper technical implementation, we think as many attorneys as necessary should have been read in to assure the soundness of the program's legal foundation. This was not done during the early phase of the program. ~~(TS//SI//NF)~~

The full history of the program also indicates that the program benefited from additional attorney read-ins. In this chapter, we described how Philbin and Goldsmith – who held differing opinions on which legal theory best supported the program – discovered serious deficiencies in Yoo's analysis and together drafted more factually accurate and legally thorough support for the program. In Chapters Five, Six, and Seven we further describe how reading in additional attorneys facilitated the grounding of the program on firmer legal footing under FISA, allowed the Department more efficiently to "scrub" Stellar Wind-derived information in FISA applications,

---

[229] As discussed in this chapter, Comey, Goldsmith, and Philbin generally agreed that Gonzales supported the Department's legal reassessment of the program. They also characterized Addington as far less supportive of their work than Gonzales. ~~(TS//SI//NF)~~

and improved the handling of Stellar Wind-related discovery issues in international terrorism prosecutions. ~~(TS//STLW//SI//OC/NF)~~

Second, we do not believe that reading in a few additional Department attorneys during the first 2 years of the program would have jeopardized national security as suggested by Gonzales, especially given the hundreds of operational personnel who were cleared into the program during the same period (see Chart 4.1). In fact, as noted above, we think the highly classified nature of the program, rather than constituting an argument for limiting the OLC read-ins to a single attorney, made the need for careful analysis and review within the Department and by the NSA only more compelling. ~~(TS//SI//NF)~~

In sum, we concluded that the departure from established OLC and Department practices resulted in legal opinions to support the program that were later determined to be flawed. We believe the strict control over the Department's access to the program undermined the role of the Department to ensure the legality of Executive Branch actions, and as discussed below, contributed to the March 2004 crisis that nearly resulted in the mass resignation of the Department's leadership. ~~(TS//SI//NF)~~

We recommend that when the Justice Department is involved with such programs in the future, the Attorney General should carefully assess whether the Department has been given adequate resources to carry out its vital function as legal advisor to the President and should aggressively seek additional resources if they are found to be insufficient. We also believe that the White House should allow the Department a sufficient number of read-ins when requested, consistent with national security considerations, to ensure that sensitive programs receive a full and careful legal review. (U)

B. The Hospital Visit (U)

The Department's reassessment of Yoo's analysis led Comey, who was exercising the powers of the Attorney General while Ashcroft was hospitalized in March 2004, to conclude that he could not certify the legality of the Stellar Wind program. In response, the President sent Gonzales and Chief of Staff Andrew Card to visit Ashcroft in the hospital to seek his certification of the program, an action Ashcroft refused to take. We believe that the way the White House handled its dispute with the Department about the program – particularly in dispatching Gonzales and Card to Ashcroft's hospital room to override Comey's decision – was troubling for several reasons. ~~(TS//SI//NF)~~

As discussed in this chapter, by March 2004, when the Presidential Authorization was set to expire again, Goldsmith had placed Gonzales and Addington on notice for several months of the Department's doubts about

the legality of aspects of the Stellar Wind program. In particular, he and Philbin had made clear that the Department questioned the legality of the collections of [redacted].[230] ~~(TS//STLW//SI//OC/NF)~~

After Attorney General Ashcroft was hospitalized and unable to fulfill his duties, the White House was informed that Deputy Attorney General Comey had assumed the Attorney General's responsibilities. We found that the assertion by some in the White House at the time that they had not been informed of the situation was subsequently contradicted by the facts. In particular, Gonzales later acknowledged that he was aware that Comey was acting as the Attorney General.[231] (U)

Before the Presidential Authorization was set to expire on March 11, Comey, who was exercising the powers of the Attorney General at the time, told top officials in the White House – including Vice President Cheney and White House Counsel Gonzales – that the Justice Department could not recertify the legality of the program as it was presently operating. The White House disagreed with the Justice Department's position, and on March 10, 2004, convened a meeting of eight congressional leaders to brief them on the Justice Department's seemingly sudden reluctance to recertify the program and on the need to continue the program. The White House did not invite anyone from the Department to this briefing to describe the basis for its advice about the legality of the program, nor did it inform the Department of its intention to hold the meeting.[232] ~~(TS//SI//NF)~~

Following this briefing, Gonzales and Card went to the hospital to ask Attorney General Ashcroft, who was in the intensive care unit recovering

---

[230] Our conclusion that Goldsmith advised Gonzales and Addington of the Department's concerns in December 2003 is supported by his contemporaneous notes of these events. In addition, although Gonzales told us that the first time he recalled hearing of these concerns in detail was in early March 2004, he did not dispute that Goldsmith had first begun to advise him of the Department's general concerns months earlier. (U)

[231] During his congressional testimony, when questioned about whether he knew that Attorney General Ashcroft's powers had been transferred to Comey, Gonzales responded, "I think that there were newspaper accounts, and that fact that Mr. Comey was the acting Attorney General is probably something I knew of." (U)

[232] On the advice of White House counsel, Gonzales declined to provide a reason to the OIG why the Department was not asked to participate in the briefing. However, when Gonzales commented on a draft of this report, he stated that the purpose of the meeting was to inform the congressional leaders that the Department had a problem with the legal basis for aspects of the program, [redacted] and that a legislative fix therefore was necessary. Gonzales stated that the purpose of the meeting was not to have a "debate" between the White House and the Department concerning the legality of the program, but rather to explore just such a legislative "fix." ~~(TS//SI//NF)~~

from surgery and according to witnesses appeared heavily medicated, to certify the program, notwithstanding Comey's stated opposition. Yet, they did not notify Comey or anyone else in the Department that they intended to take this action. Their attempt to have Ashcroft recertify the program did not succeed. Ashcroft told them from his hospital bed that he supported the Department's legal position, but that in any event he was not the Attorney General at the time – Comey was. (U)

Gonzales stated that even if he knew that Ashcroft was aware of Comey's opposition to recertifying the program, Gonzales would still have wanted to speak with Ashcroft because he believed Ashcroft still retained the authority to certify the program. Gonzales testified before the Senate Judiciary Committee in July 2007 that although there was concern over Ashcroft's condition, "We would not have sought nor did we intend to get any approval from General Ashcroft if in fact he wasn't fully competent to make that decision." Gonzales also testified, "There's no governing legal principle that says that Mr. Ashcroft, if he decided he felt better, could decide, 'I'm feeling better and I can make this decision, and I'm going to make this decision.'" (U)

We found this explanation and the way the White House handled the dispute to be troubling. Rather, we agree with Director Mueller's observation, as recorded in his program log following his meeting with Card on March 11, 2004, that the failure to have Department of Justice representation at the congressional briefing and the attempt to have Ashcroft certify the Authorization by overruling Comey "gave the strong perception that the [White House] was trying to do an end run around the Acting [Attorney General] whom they knew to have serious concerns as to the legality of portions of the program." ~~(TS//SI//NF)~~

At a minimum, we would have expected the White House to alert Comey directly that it planned to brief the congressional leaders on the Department's position and that it intended to seek Ashcroft's approval of the program despite Comey and Goldsmith's stated legal position against continuing certain activities under the program. Instead, White House officials briefed congressional leaders and sought to have Attorney General Ashcroft recertify the program from his hospital bed without any notice to Comey or anyone else at the Department. We believe these actions gave the appearance of an "end run" around the ranking Justice Department official with whom they disagreed. ~~(TS//SI//NF)~~

C. Recertification of the Presidential Authorization and Modification of the Program (U)

As described in this chapter, the Department had notified Gonzales and Addington of its concerns about the legality of aspects of the program

for several months. In fact, the Department had made clear to the White House in December 2003 and more emphatically in a series of meetings in March 2004 that it believed that aspects of the program could not be legally supported in their existing form. Comey and Goldsmith were clear in their advice to the President and other White House officials. At the hospital, Ashcroft also expressed deep concern [redacted] and told Gonzales and Card that he supported the position of his subordinates. We believe that Ashcroft acted admirably under arduous circumstances. ~~(TS//STLW//SI//OC/NF)~~

Despite the legal concerns uniformly expressed by senior Department of Justice leaders, the White House, through White House Counsel Gonzales, recertified the Authorization, allowing the program to continue substantively unchanged. ~~(TS//SI//NF)~~

Only after Mueller, Comey, and other senior Department and FBI officials made known their intent to resign if the White House continued the program unchanged, despite the Department's conclusion that aspects of the program could not be legally supported, did the President direct that the issue be resolved, and the program be modified to address the Department's legal concerns. Because we were unable to interview key White House officials, we could not determine for certain what caused the White House to change its position and modify the program, although the prospect of mass resignations at the Department and the FBI appears to have been a significant factor in this decision.[233] According to Comey, the President raised a concern that he was hearing about these problems at the last minute, and the President thought it was not fair that he was not told earlier about the Department's legal position. In fact, as Comey informed the President, the President's staff had been advised of these issues "for weeks." ~~(TS//SI//NF)~~

Finally, we believe that the Department and FBI officials who resisted the pressure to recertify the Stellar Wind program because of their belief that aspects of the program were not legally supportable acted courageously and at significant professional risk. We believe that this action by Department and FBI officials – particularly Ashcroft, Comey, Mueller,

---

[233] For instance, we found it significant that on March 16, 2004, White House Counsel Gonzales, who had to make a recommendation to the President about how to proceed with the program in view of the Department's conclusion that legal support for [redacted] called Director Mueller to ask him whether he would resign if the President did not [redacted] Mueller responded that he "would have to give it serious consideration if the President decided to go ahead in the face of DOJ's finding." [redacted] ~~(TS//STLW//SI//OC/NF)~~

Goldsmith, Philbin, and Baker – was in accord with the highest professional standards of the Justice Department. ~~(TS//SI//NF)~~

CHAPTER FIVE
STELLAR WIND PROGRAM'S TRANSITION TO FISA AUTHORITY
(JUNE 2004 THROUGH AUGUST 2007)

In this chapter we examine the transition in stages of the Stellar Wind program from presidential authority to FISA authority. We first describe the FISA Court's approval in July 2004 of the government's application to acquire foreign intelligence information through the collection of bulk e-mail meta data (basket 3 information). This application was based on a legal theory related to FISA's pen register and trap and trace device provisions. We next discuss the government's successful May 2006 application to the FISA Court for an order to obtain bulk telephony meta data (basket 2 information) by the production of business records by certain telecommunications carriers. We then describe the government's interaction with the FISA Court to place under FISA the government's authority to intercept the content of certain communications involving both domestic and foreign telephone numbers and e-mail addresses (basket 1 information). Finally, we summarize legislation enacted in August 2007 and July 2008 to amend FISA to address, among other concerns, the difficulty the government encountered in obtaining FISA authority for content collection, as well as the government's contention that certain provisions of FISA had failed to keep pace with changes in telecommunications technology. ~~(TS//STLW//SI//OC/NF)~~

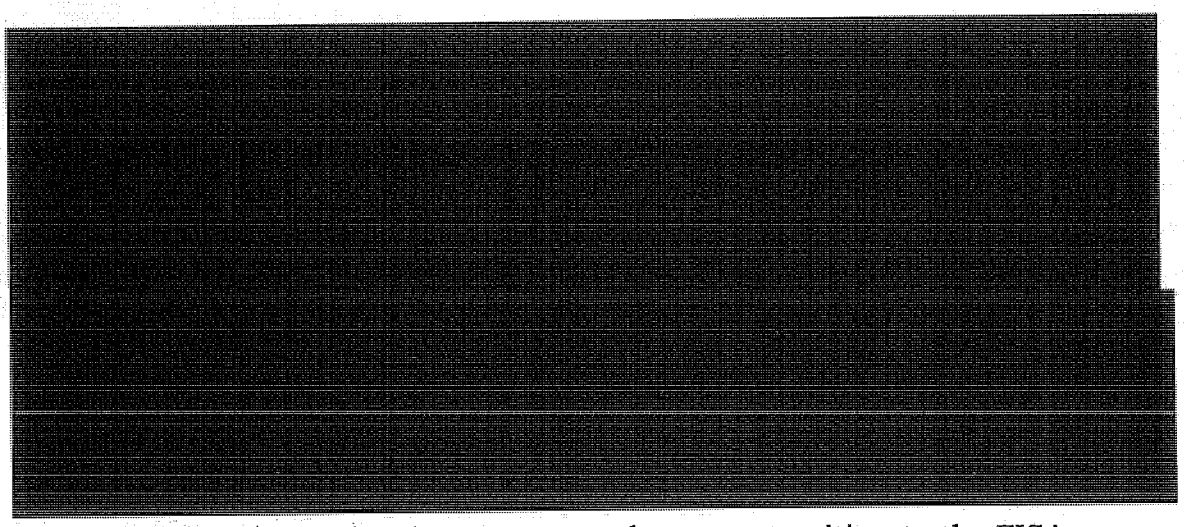
I. E-Mail Meta Data Collection Under FISA ~~(TS//SI//NF)~~

A. Application and FISA Court Order (U)

[redacted] The FISA Court granted this authority on July 14, 2004 [redacted] ~~(TS//STLW//SI//OC/NF)~~

1. Decision to Seek a Pen Register and Trap and Trace (PR/TT) Order from the FISA Court ~~(TS//SI//NF)~~

[redacted]



Philbin told us that he encountered some opposition to the FISA approach from Counsel to the Vice President David Addington, who argued that the FISA Court was unconstitutional and questioned the need to seek its authorization for e-mail meta data collection. Philbin said that he responded that obtaining an order from the FISA Court was "ironclad safe." Baker recalled attending at least one meeting at the White House with White House Counsel Gonzales and Addington to discuss whether to seek an order from the FISA Court based on FISA's pen register and trap and trace device provisions (a PR/TT Order) and how the FISA Court should be approached to obtain such an order. Baker stated that during the meeting Addington said, "We are one bomb away from getting rid of this obnoxious Court." Baker said Addington also stressed to him that there "is a lot riding on your [Baker's] relationship with this Court." ~~(TS//STLW//SI//OC/NF)~~

In contrast, Hayden told us that he did not have any concerns about transitioning the bulk e-mail meta data collection to FISA authority and was enthusiastic about the move. Hayden stated that while he believed the President had the authority to collect the bulk meta data for the NSA to conduct meta data analysis, he believes that involving an additional branch of government in the activity provided some clarity on this subject. ~~(TS//STLW//SI//OC/NF)~~

Gonzales told us that he did not recall much about the process of filing the application with the FISA Court to obtain e-mail meta data through a PR/TT Order, but stated that there may have been individuals at the White House who expressed concern that seeking the Order from the FISA Court was not a good idea. However, Gonzales told us that he was supportive of seeking the Order [redacted] He stated that he relied on what the intelligence professionals told him and that he would not have supported the PR/TT application if NSA Director Hayden and others did not believe the collection under the PR/TT Order provided the coverage necessary to protect the nation [redacted] Gonzales

also told us that there was concern at the White House that filing the PR/TT application could lead to an unauthorized disclosure of the program. ~~(TS//STLW//SI//OC/NF)~~

2. Briefing for Judge Kollar-Kotelly (U)

In [redacted] Baker, Philbin, and Goldsmith met with Gonzales and Addington at the White House to discuss how to approach Judge Kollar-Kotelly concerning the proposed PR/TT application, and it was decided to give her a "presentation" about the application. The presentation was provided to Judge Kollar-Kotelly on [redacted] Present were Attorney General Ashcroft, Central Intelligence Agency Director George Tenet, FBI Director Mueller, Hayden, Gonzales, OLC Assistant Attorney General Goldsmith, Philbin, Baker, and Director of the Terrorist Threat Integration Center (TTIC) John Brennan. According to an agenda of the briefing, and as confirmed to the OIG, the presentation was given in three parts. First, Mueller, Tenet, and Brennan described the nature of the terrorist threat facing the United States, including concerns of [redacted] Second, Hayden described the technical aspects of the proposed bulk e-mail meta data collection, including how the information was to be collected, archived, queried, and minimized. This portion of the presentation stressed that the NSA required the collection of meta data in bulk to maximize analytic capabilities through contact chaining [redacted] to identify terrorist communications.[234] Third, Philbin explained the government's legal argument that FISA authorized the Court to approve a broad application to collect e-mail meta data under the statute's pen register and trap and trace provisions. ~~(TS//STLW//SI//OC/NF)~~

[redacted] ~~(TS//SI//NF)~~

3. The PR/TT Application ~~(TS//SI//NF)~~

Philbin, Baker, and at least two Office of Legal Counsel attorneys assumed primary responsibility for drafting the PR/TT application to the FISA Court and a memorandum of law in support of the application.[235]

---

[234] The agenda refers to the "needle in haystack" metaphor to illustrate the need for bulk collection, noting "must transform streams of hay into haystack that can later be searched." ~~(TS//SI//NF)~~

[235] The application package, captioned [redacted] consisted of the application; a proposed order authorizing the collection activity and secondary orders mandating carriers to cooperate; a declaration of NSA Director Hayden explaining the technical aspects of the (Cont'd.)

Baker said that Judge Kollar-Kotelly was given a "read-ahead copy" of the application, since it was standard practice to give the FISA Court draft applications for review. ~~(TS//SI//NF)~~

The final application was filed [redacted] A short addendum to the application filed [redacted] it sought authorization from the FISA Court to collect. ~~(TS//SI//NF)~~

The objective of the application was to secure authority under FISA to collect [redacted] bulk e-mail meta data [redacted] the meta data to be collected under FISA authority would be stored in a database. According to the application, queries could be run against the database to identify [redacted] by looking for contacts with other individuals reasonably suspected to be [redacted] and to reveal communications links between such operatives. The resulting analytical products would then be tipped out as leads to the FBI and other elements of the U.S. Intelligence Community to find members of [redacted] disrupt their activities, and prevent future terrorist attacks in the United States.[236] ~~(TS//STLW//SI//OC/NF)~~

The Justice Department constructed its legal argument for this novel use of pen register and trap and trace devices around traditional authorities provided under FISA. Specifically, 50 U.S.C. § 1842(a)(1) authorizes the Attorney General or other designated government attorney to apply

> for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect

---

proposed e-mail meta data collection and identifying the government official seeking to use the pen register and trap and trace devices covered by the application for purposes of 50 U.S.C. § 1842(c)(1); a declaration of Director of Central Intelligence Tenet describing the threat posed by [redacted]; a certification from Attorney General Ashcroft stating that the information likely to be obtained from the pen register and trap and trace devices was relevant to an ongoing investigation to protect against international terrorism, as required by 50 U.S.C. § 1842(c); and a memorandum of law and fact in support of the application. ~~(TS//SI//NF)~~

[236] The application emphasized that Internet e-mail is one of the primary methods by which [redacted] communicate. The memorandum of law in support of the application stated that Internet e-mail is particularly attractive to terrorists [redacted] ~~(TS//SI//NF)~~

> against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order. ~~(TS//SI//NF)~~

FISA incorporated the definitions of the terms "pen register" and "trap and trace device" from 18 U.S.C. § 3127. Thus, FISA adopted as the definition of a "pen register"

> a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication. ~~(TS//SI//NF)~~

18 U.S.C. § 3127(3). FISA also adopted as the definition of a "trap and trace device"

> a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication. ~~(TS//SI//NF)~~

18 U.S.C. § 3127(4).

In its application the government argued that the NSA's proposed collection of meta data met the requirements of FISA by noting that the meta data sought comported with the "dialing, routing, addressing, or signaling information" type of data described in FISA's definitions of pen registers and trap and trace devices. The government also noted that nothing in these definitions required that the "instrument" or "facility" on which the device is placed carry communications of only a single user rather than multiple users. ~~(TS//SI//NF)~~

The government next argued that the information likely to be obtained from the pen register and trap and trace devices was relevant to an ongoing investigation to protect against international terrorism, as certified by the Attorney General under 50 U.S.C. § 1842(c). In support of this "certification of relevance" the government stated that the FBI was conducting more than [redacted] ~~(TS//SI//NF)~~

The government acknowledged that "the overwhelming majority of communications from which meta data will be collected will not be associated with [redacted]." However, the government maintained that FISA did not impose any requirement to tailor collection precisely to obtain only communications that are strictly relevant to the investigation. The government argued that, in any event, "the tailoring analysis must be informed by the balance between the overwhelming national security interest at stake . . . and the minimal intrusion into privacy interests that will be implicated by collecting meta data – especially meta data that will never be seen by a human being unless a connection to a terrorist-associated e-mail is found." ~~(TS//SI//NF)~~

The government also stated that the NSA needed to collect meta data in bulk in order to effectively use analytic tools such as contact chaining [redacted] that would enable the NSA to discover enemy communications. This argument echoed a premise many officials told us about the nature of intelligence gathering in general. For example, Baker likened the search for useful intelligence, particularly in the meta data context, to finding a needle in a haystack, stating, "the only way to find the needle is to have the haystack." Gonzales argued that "to connect the dots you first have to collect the dots." ~~(TS//SI//NF)~~

The application and supporting documents described the [redacted] types of e-mail meta data NSA sought authority to collect:

[redacted]

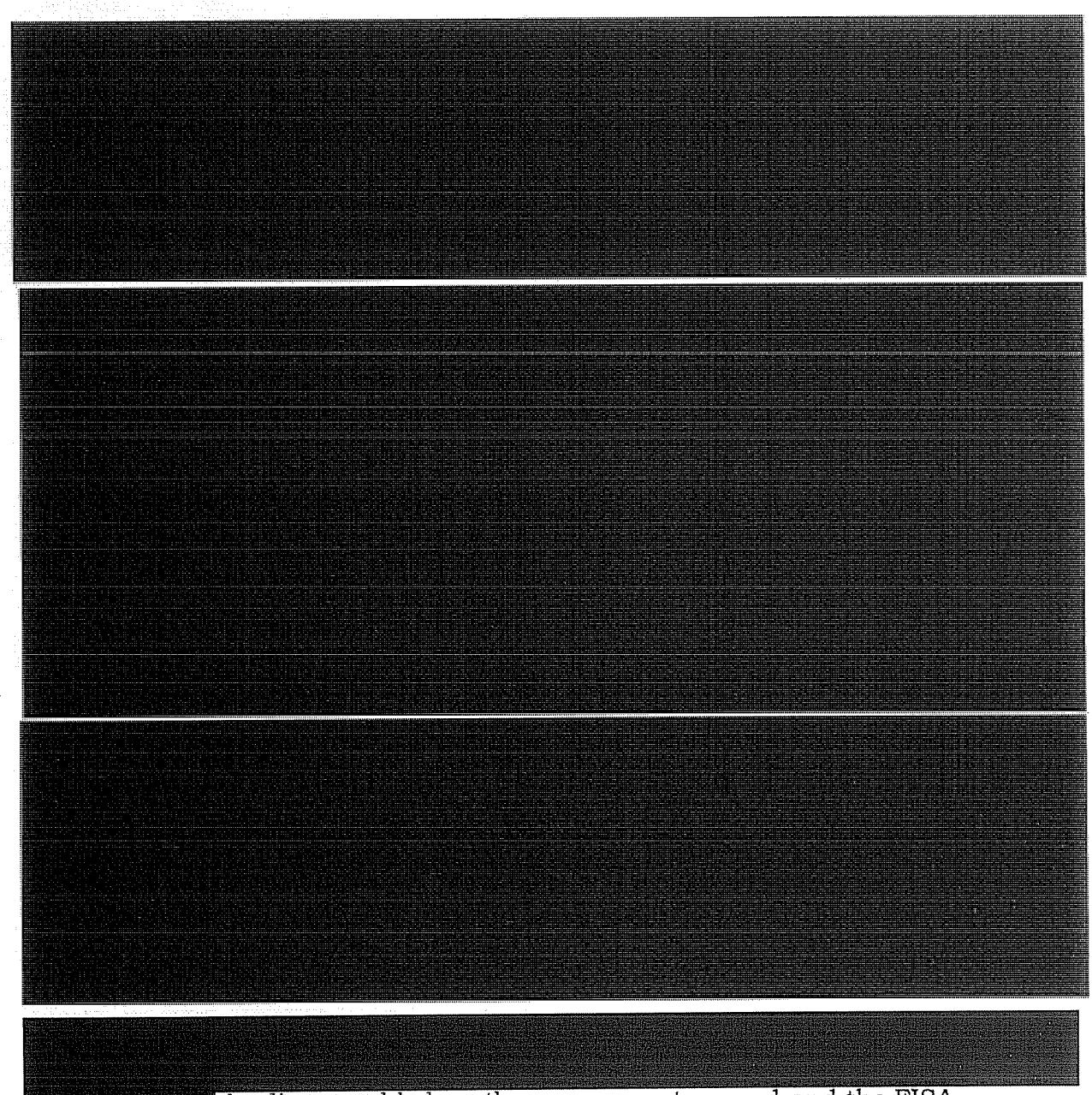
The application requested that the NSA be authorized to collect this meta data [redacted] were described as follows:

[redacted]

The application represented that for most of the proposed collection on [redacted] it was "overwhelmingly likely" that at least one end of the transmitted communication either originated in or was destined for locations outside the United States, and that in some cases both ends of the communication were entirely overseas.[237] However, the government acknowledged that [redacted] (~~TS//SI//NF~~)

[redacted]

[237] [redacted]



As discussed below, the government argued and the FISA Court ultimately agreed that the above-described collection satisfied the definitions of pen register and trap and trace devices under FISA and Title 18. See 50 U.S.C. § 1841(2); 18 U.S.C. § 3127(3) & (4). ~~(TS//SI//NF)~~

The application also explained the proposed archiving and querying process. According to the application, the collected meta data would be stored in a secure NSA network accessible only through two administrative login accounts and by specially-cleared meta data archive system administrators. Each time the database was accessed, the retrieval request would be recorded for auditing purposes. ~~(TS//SI//NF)~~

The application proposed allowing 10 NSA analysts access to the database.[238] The NSA analysts were to be briefed by the NSA Office of General Counsel concerning the circumstances under which the database could be queried, and all queries would have to be approved by one of seven senior NSA officials.[239] ~~(TS//SI//NF)~~

The application explained that the bulk collection would be queried with particular e-mail addresses in order to conduct chaining [redacted] The application proposed that queries of the e-mail meta data archive would be performed when the e-mail address met the following standard:

> based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known e-mail address is associated with [redacted]

[redacted] Under the PR/TT application, the government proposed that it be authorized under FISA [redacted] to use the reasonable articulable suspicion standard to query the database with specific addressing information [redacted]
(TS//STLW//SI//OC/NF)

In addition, the NSA proposed applying the minimization procedures in the United States Signals Intelligence Directive 18 (USSID 18) to minimize the information reported concerning U.S. persons. According to the application, compliance with these minimization procedures would be

---

238 At the government's request the number of NSA analysts was increased to 15 when the Order was renewed [redacted] ~~(TS//SI//NF)~~

239 When it granted the government's application, the FISA Court noted that in conventional pen register and trap and trace surveillances a court first reviews the application before a particular e-mail account can be targeted. The FISA Court stressed the importance of the NSA Office of General Counsel's obligation to ensure that the legal adequacy for such queries was met. ~~(TS//SI//NF)~~

monitored by the NSA's Inspector General and General Counsel. The government also proposed that in each renewal application the NSA would report to the FISA Court on queries that were made during the prior period and the application of the reasonable articulable suspicion standard for determining that queried addresses were terrorist-related. ~~(TS//SI//NF)~~

The application and supporting documents explained how the NSA intended to use the collected meta data. The NSA sought to use the meta data [redacted] to apply sophisticated algorithms to develop contact chaining [redacted].[240] In the application, the NSA estimated that through external intelligence gathering and internal analysis it would meet the proposed querying standard on average less than once a day. The NSA further estimated that these queries would generate approximately 400 tips to the FBI and CIA per year.[241] Of these tips to the FBI and CIA, the NSA projected that 25 percent would include U.S. person information, amounting to leads including information on about "four to five U.S. persons each month." ~~(TS//SI//NF)~~

4. Judge Kollar-Kotelly Raises Questions about PR/TT Application ~~(TS//SI//NF)~~

On [redacted] Judge Kollar-Kotelly wrote Baker to inform him that she was considering the application and was in the process of preparing an opinion and order in response to it. She wrote that before the opinion and Order could be completed, however, she required written responses to two questions:

(1) Apart from the First Amendment proviso in the statute (50 U.S.C. § 1842(a)(1), (c)(2)), what are the general First Amendment implications of collecting and retaining this large volume of information that is derived, in part, from the communications of U.S. persons?

(2) For how long would the information collected under this authority continue to be of operational value to the counter-terrorism investigation(s) for which it would be collected? ~~(TS//SI//NF)~~

Baker responded in a letter to the FISA Court on [redacted] Concerning the first question, Baker's letter asserted that the proposed

---

240 These analytic tools are discussed in Chapter Three. (U)

241 The NSA arrived at this estimate based on the assumption that each query could be expected to generate [redacted] e-mail addresses "one level out," and [redacted] addresses "two levels out." The overall number of direct and indirect contacts with the initial seed address would be significantly reduced using "analytical tradecraft." ~~(TS//SI//NF)~~

collection activity was consistent with the First Amendment and that he could find no reported decisions holding that the use of pen register and trap and trace devices violated the First Amendment. ~~(TS//SI//NF)~~

In his letter, Baker argued that although the meta data collection would include entirely innocent communications, a good-faith investigation does not violate the First Amendment simply because it is "'broa[d] in scope'" (quoting *Laird v. Tatum*, 408 U.S. 1, 10 (1972)). He also wrote that the use of the collected meta data would be "narrowly constrained" because the querying standard for the meta data would be subject to a "reasonable articulable suspicion" of a nexus to [redacted] ~~(TS//SI//NF)~~

Regarding Judge Kollar-Kotelly's second question concerning how long the collected meta data would continue to be of operational value, Baker wrote that, based on the analytic judgment of the NSA, such information would continue to be relevant to [redacted] for at least 18 months. Baker also advised that the NSA believed the e-mail meta data would continue to retain operational value beyond 18 months, but that it should be stored "off-line" and be accessible to queries only by a specially-cleared administrator. Baker proposed that 3 years after the 18-month timeframe, or 4½ years after it is first collected, the meta data could be destroyed.[242] ~~(TS//SI//NF)~~

5. FISA Court Order (U)

In response to the application and follow-up questions, on July 14, 2004, Judge Kollar-Kotelly signed a Pen Register and Trap and Trace Opinion and Order based on her findings that the proposed collection of e-mail meta data and the government's proposed controls over and dissemination of this information satisfied the requirements of FISA. ~~(TS//HCS//SI//NF)~~

The Order granted the government's application in all key respects. It approved for a period of 90 days the collection within the United States of e-mail meta data [redacted] The Order also required the government to comply with certain additional restrictions and procedures either adapted from or not originally proposed in the application. ~~(TS//HCS//SI//NF)~~

In the Order, the Court found that the information to be collected was "dialing, routing, addressing, or signaling information" that did not include

---

[242] On [redacted] the FISA Court issued an order authorizing the NSA to maintain bulk meta data on-line for 4½ years after which time it must be destroyed. According to the NSA Office of General Counsel, the NSA still follows this retention procedure. ~~(TS//HCS//SI//NF)~~

the contents of any communication. The Court stressed that it was only authorizing collection of the [redacted] categories of information delineated in the application, but acknowledged that additional information "could be gleaned" from that meta data. [redacted] The Court found that the means by which the [redacted] categories of meta data were to be collected met the FISA definition of a "pen register," and that the means for collecting the [redacted] category of meta data satisfied the FISA definition of a "trap and trace device." See 18 U.S.C. § 3127(3) & (4), as incorporated in FISA at 50 U.S.C. § 1841(2). ~~(TS//HCS//SI//NF)~~

The Court further found that the government satisfied FISA's requirement that the application certify that the information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism. The Court concluded that, "under the circumstances of this case, the applicable relevance standard does not require a statistical 'tight fit' between the volume of proposed collection and the much smaller proportion of information that will be directly relevant to [redacted] FBI investigations."[243] ~~(TS//HCS//SI//NF)~~

The Court also agreed with the government's position that the privacy interest at stake in the collection of e-mail meta data did not rise to the "stature protected by the Fourth Amendment," and that the nature of the intrusion was mitigated by the restrictions on accessing and disseminating the information, only a small percentage of which would be seen by any person. ~~(TS//HCS//SI//NF)~~

In sum, the Court concluded that the use of pen register and trap and trace devices to collect e-mail meta data would not violate the First Amendment, stating that

> the bulk collection proposed in this case is analogous to suspicionless searches or seizures that have been upheld under the Fourth Amendment in that the Government's need is compelling and immediate, the intrusion on individual privacy interests is limited, and bulk collection appears to be a reasonably effective means of detecting and monitoring [redacted]

---

[243] The Court cautioned that its ruling with regard to the breadth of the meta data collection should not be construed as precedent for similar collections of the full content of communications under the electronic surveillance provisions of FISA. The Court noted important differences in the two types of collection, including the fact that overbroad electronic surveillance requires a showing of probable cause to believe the target is an agent of a foreign power, while the bulk meta data collection under FISA's pen register and trap and trace device provisions merely requires a showing that the overbroad collection is justified as necessary to discover unknown [redacted] persons. The Court also contrasted the high privacy interests at stake with respect to content communications with the absence of a privacy interest in meta data. ~~(TS//SI//NF)~~

[redacted] related operatives and thereby obtaining information likely to be [redacted] to ongoing FBI investigations. ~~(TS//HCS//SI//NF)~~

However, the Court also was concerned that "the extremely broad nature of this collection carries with it a heightened risk that collected information could be subject to various forms of misuse, potentially involving abridgement of First Amendment rights of innocent persons." The Court noted that under 50 U.S.C. § 1842(c)(2), pen register and trap and trace information about the communications of a U.S. person cannot be targeted for collection unless it is relevant to an investigation that is not solely based upon the First Amendment. Therefore, the Court ordered that the NSA modify its criterion for querying the archived data by inserting the following underlined language, as shown below:

> [redacted] will qualify as a seed [redacted] only if NSA concludes, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known e-mail address is associated with [redacted] provided, however, that an [redacted] believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution. ~~(TS//HCS//SI//NF)~~

Regarding the storage, accessing, and disseminating of the e-mail meta data obtained by the NSA, the Court ordered that the NSA must store the information in a manner that ensures it is not commingled with other data, and must "generate a log of auditing information for each occasion when the information is accessed, to include the . . . retrieval request." The Court further ordered that the e-mail meta data "shall be accessed only through queries using the contact chaining [redacted]" as described by the NSA in the government's application. ~~(TS//HCS//SI//NF)~~

The Court noted the "distinctive legal considerations" involved in implementing the authority the Court was vesting in the NSA. Specifically, the Court observed that conventional pen register and trap and trace surveillance required judicial review before any particular e-mail account could be targeted. However, by granting the government's application, the Court noted that the NSA's decision to target an e-mail address (sometimes referred to as a "seed [redacted]") would be made without judicial review. Therefore, the Court ordered that the NSA's Office of General Counsel would be responsible for training analysts to comply with querying standards and

other procedures and "to review the legal adequacy for the basis of such queries, including the First Amendment proviso . . . ." ~~(TS//HCS//SI//NF)~~

As suggested by Baker in his [redacted] response to Judge Kollar-Kotelly's inquiry regarding the useful life of the collected data, the Court ordered that the e-mail meta data shall be available for 18 months for querying. The Court further ordered that after the 18-month period, the data must be transferred to an "off-line" tape system from which it could still be accessed for querying upon approval of the NSA officials authorized to approve queries, and that such meta data must be destroyed 4½ years after initially collected. ~~(TS//HCS//SI//NF)~~

The Court's Order was set to expire after 90 days. The Court required that any application to renew or reinstate the authority granted in the Order must include: a report discussing queries made since the prior application and the NSA's application of the requisite legal standard to those queries; detailed information regarding [redacted] proposed to be added to the authority granted under the Order; any changes to the description of the [redacted] described in the Order or the nature of the communications [redacted] and any changes to the proposed means of collection, including to the [redacted] of the pen register and trap and trace devices [redacted]
~~(TS//HCS//SI//NF)~~

Finally, the Court issued separate orders [redacted] to assist the NSA with the installation and use of the pen register and trap and trace devices and to maintain the secrecy of the NSA's activities. These orders [redacted] called "secondary orders," [redacted] The NSA was directed to compensate the carriers for all assistance provided in connection with the PR/TT Order.
~~(TS//HCS//SI//NF)~~

Baker and other witnesses told us that obtaining the Order was seen by the Department as a great success, and that there was general agreement that the government had secured all the authority it sought to conduct the bulk e-mail meta data collection. [redacted] Comey told us that obtaining the Order from the FISA Court also provided an "air of legitimacy" to the program.[244] ~~(TS//STLW//SI//OC/NF)~~

---

[244] Comey and others informally referred to the PR/TT Order as "the mother of all pen registers." ~~(TS//SI//NF)~~

B. President Orders Limited Use [redacted] (~~TS//STLW//SI//OC/NF~~)

E-mail meta data collection under FISA pen register authority began when the PR/TT Order took effect on July 14, 2004. As required by the Order, the data was placed in its own database or "realm." [redacted]

~~(TS//STLW//SI//OC/NF)~~

We discuss below the President's directive and the OLC memorandum that was drafted to analyze its legality. ~~(TS//STLW//SI//OC/NF)~~

1. The President's August 9, 2004, Memorandum to the Secretary of Defense ~~(TS//SI//NF)~~

On August 9, 2004, the same day a routine Presidential Authorization was issued to continue Stellar Wind, the President sent a separate memorandum to the Secretary of Defense regarding the use of the e-mail meta data collected [redacted] The memorandum directed the Secretary of Defense that, consistent with the August 9, 2004, Presidential Authorization (and any successor Presidential Authorizations), the NSA was authorized to [redacted] e-mail meta data [redacted] when there was a reasonable articulable suspicion that (1) a party to the communication belonged to [redacted] and (2) the purpose of the search was to produce foreign intelligence information concerning threats [redacted][245] ~~(TS//STLW//SI//OC/NF)~~

[245] The President's Memorandum provided that the authority to conduct such searches was to terminate on September 23, 2004. In the September 17, 2004, Presidential Authorization, this authority was extended until November 18, 2004. ~~(TS//STLW//SI//OC/NF)~~

2. Office of Legal Counsel Determines [redacted]

~~(TS//STLW//SI//OC/NF)~~

Jack Goldsmith resigned as Assistant Attorney General for the Office of Legal Counsel on July 30, 2004. Goldsmith was replaced by Daniel Levin, who served as the Acting Assistant Attorney General for OLC until February 2005. (U)

During late 2004, at the request of Comey and Ashcroft, Levin began work on an OLC memorandum addressing whether it would be lawful for the NSA to analyze the e-mail meta data collected [redacted] b1, b3, b7E

(TS//STLW//SI//OC/NF) [redacted]

---

246 The [redacted] e-mail meta data has since been placed on tape and is being held by the NSA Office of General Counsel pursuant to a preservation order. ~~(TS//STLW//SI//OC/NF)~~

247 The final version of the OLC memorandum was signed by Levin on February 4, 2005. Levin told the OIG that a "policy decision" was made to limit application of the memorandum to the specific purpose [redacted] However, Levin stated that, based on his analysis of the issue, he believed that [redacted] (Cont'd.)

Thus, the President asserted extrajudicial authority to order the further use of e-mail meta data collected under Stellar Wind for the limited purpose described in his August 9 memorandum. The FISA Court was notified of this action, although the government did not seek its permission. ~~(TS//STLW//SI//OC/NF)~~

C. Non-Compliance with PR/TT Order ~~(TS//SI//NF)~~

As with other orders issued under FISA, the PR/TT Order was renewed every 90 days. During the early renewals, two major instances of non-compliance were brought to the FISA Court's attention. As described below, these violations of the Order resulted primarily from the NSA senior officials' failure to adequately communicate the technical requirements of the Order to the NSA operators tasked with implementing them, and from miscommunications among the FISA Court, the Justice Department, and the NSA concerning certain legal issues. ~~(TS//SI//NF)~~

1. Filtering Violations ~~(TS//SI//NF)~~

On (b)(3) OIPR filed a Notice of Compliance Incidents with the FISA Court. In the Notice, Baker stated that the compliance incidents cited in the Notice "raise compliance issues with about (b)(3) of the collection authorized by the Court."[248] The Notice included as an attachment a letter from NSA General Counsel Robert Deitz to Baker describing incidents that led to "unauthorized collection." Deitz learned of these incidents on (b)(3).[249] ~~(TS//SI//NF)~~

(b)(1), (b)(3)

(b)(1), (b)(3) could be queried for any purpose. Levin told us that, other than Addington, no one else was pushing to broaden the memorandum's application. ~~(TS//STLW//SI//OC/NF)~~

[248] Subsequent filings indicate that (b)(3) of overall collections under the Order were affected by the violations. ~~(TS//SI//NF)~~

[249] One tipper that was based on this unauthorized collection was disseminated as a lead to the FBI but was subsequently retracted. ~~(TS//SI//NF)~~

(b)(1), (b)(3)

(Cont'd.)

(b)(1), (b)(3)

Baker told us that Judge Kollar-Kotelly was "not happy" about the violation. On (b)(3), (b)(1) the FISA Court issued an Order Regarding (b)(1), (b)(3) (Compliance Order). The Court wrote that the "NSA violated its own proposed limitations, which were attested to by its Director and, at the government's invitation, adopted as provisions of the orders of this Court." The Court found that the violations "resulted from deliberate actions by NSA personnel," as distinguished from technical failures. The Court stated it was also troubled by the duration of the violations, which extended from July 14 through (b)(3), (b)(1) and that the Court was reluctant to issue a renewal of the PR/TT Order as to (b)(1), (b)(3) ~~(TS//SI//NF)~~

That same day, the Court issued an Order to address (b)(1), (b)(3) (Order Regarding Required Information for Authorities Involving (b)(1), (b)(3), requiring that any application for renewal or reinstatement of PR/TT surveillance authorities (b)(1), (b)(3) be accompanied by a sworn declaration by the Secretary of Defense attesting to the state of compliance with the PR/TT Order and a description of the procedures that would be used to ensure compliance. ~~(TS//SI//NF)~~

On (b)(1), (b)(3) the government moved for an extension of time (until (b)(1), (b)(3)) within which to provide the Secretary of Defense's declaration. The motion, which the Court granted, assured the Court that surveillance (b)(1), (b)(3) had been terminated on (b)(1), (b)(3) and that on the NSA had moved to a separate database all meta data obtained (b)(1), (b)(3) through (b)(1), (b)(3) The NSA also represented that it reconstructed its contact chaining database using only properly obtained meta data and purged the unauthorized meta data from the system. ~~(TS//SI//NF)~~

A declaration by NSA Director Hayden accompanying the government's motion stated a total of (b) (1) e-mail addresses were tipped as leads to the FBI and CIA during the violation period and that (b) (1) of these leads may have come from the unauthorized collection. Hayden wrote that

(b)(1), (b)(3)

this lead was purged from the FBI's and CIA's databases on [redacted] ~~(TS//SI//NF)~~

The NSA Office of the Inspector General subsequently issued a report on its investigation of the unauthorized collections. The NSA OIG report stated that the filtering violations "probably led to actual unauthorized collection, but we have not been able to determine the extent of such collection, and we are not certain that we will be able to do so." The report further stated that the collection program under PR/TT Order authority was [redacted] ~~(TS//STLW//HCS//SI//OC/NF)~~

The report concluded that "there were systemic management failures within both [redacted] within the Signals Intelligence Directorate (SID)], and a complete lack of program management with regard to collection." The report stated that while the training provided by the NSA Office of General Counsel was "vigorous, conscientious, and compliant with the July 14 Order, it was inadequate in scope." ~~(TS//STLW//HCS//SI//OC/NF)~~

According to the report, the NSA removed as much of the tainted collection from the PR/TT database as possible. The NSA was unable to segregate unauthorized collection from [redacted] so it rebuilt that portion of the PR/TT database from [redacted] (the day after the violation was discovered), forward. Moreover, according to the NSA OIG report, analytical personnel were restricted from accessing the unauthorized meta data. ~~(TS//STLW//HCS//SI//OC/NF)~~

2. FISA Court Renews PR/TT Order ~~(TS//SI//NF)~~

The FISA Court's PR/TT Order expired on [redacted] On that date the government filed its first renewal application. The Renewal Application sought authorization to collect e-mail meta data on [redacted] and stated that the NSA had fully complied with the PR/TT Order with respect to [redacted] The government did not seek reauthorization for collection [redacted] due to a variety of operational reasons which the application did not specify. ~~(TS//SI//NF)~~

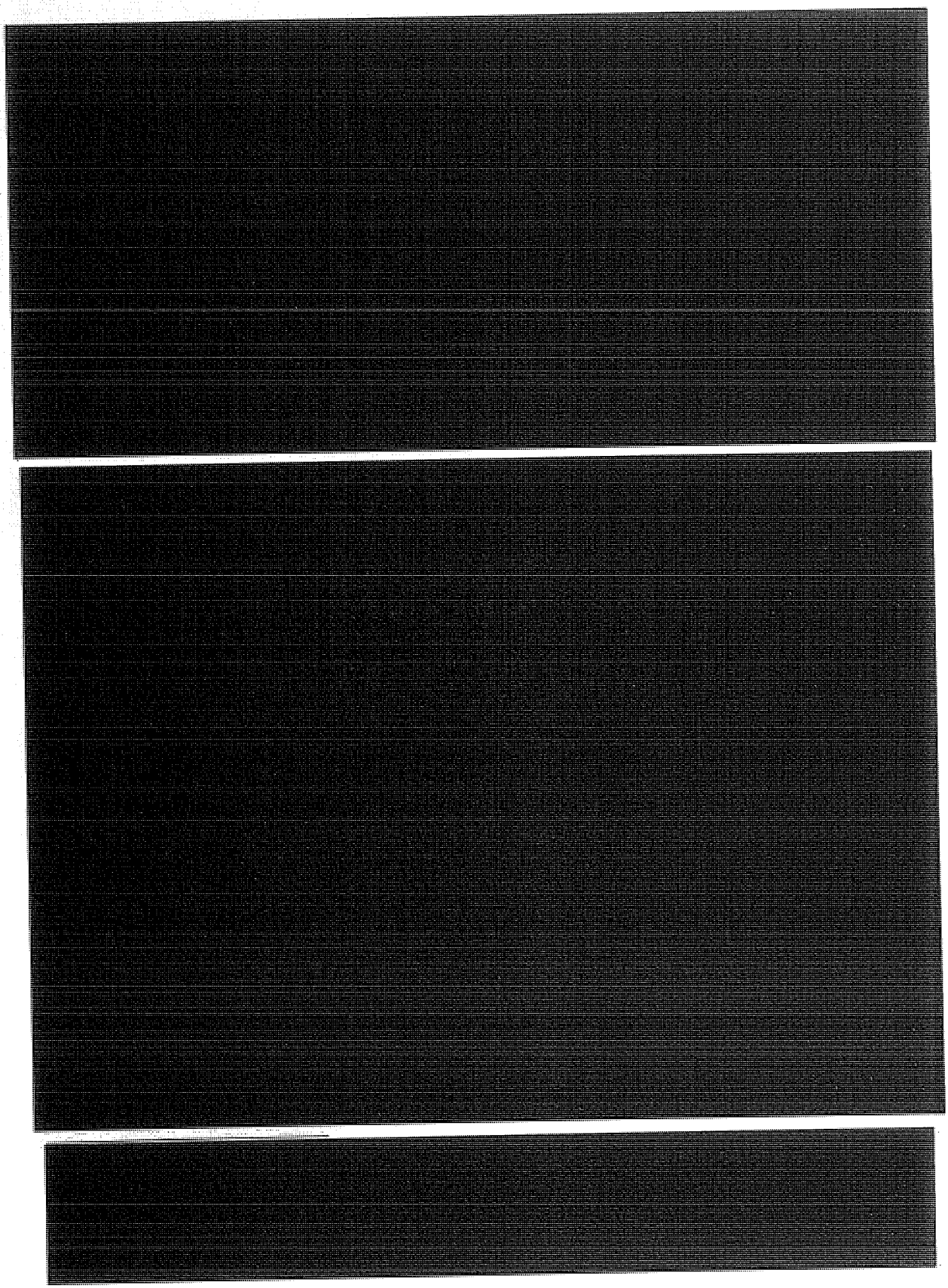
Judge Kollar-Kotelly signed the Renewal Order on [redacted] authorizing through [redacted] the use of pen register and trap and trace devices at [redacted] to collect e-mail meta data. The Renewal Order and the original Order were similar in most respects. However, in the Renewal Order the Court required the NSA to submit reports every 30 days concerning queries made since the prior report and describing any changes made to [redacted] and the [redacted] [redacted].[251] (~~TS//SI//NF~~)

3. [redacted]

Baker told us that during one of his "oversight" visits to the NSA following the FISA Court's PR/TT Order, he was given a demonstration of how the NSA analysts processed the e-mail meta data, including an explanation of how e-mail meta data is collected and queried. Baker said he was informed that among the pieces of data that might be used to meet the reasonable articulable standard for querying the e-mail meta data [redacted] (~~TS//STLW//SI//OC/NF~~) [redacted]

[251] In the initial PR/TT Order, the Court required such a report only upon the government's submission of a renewal application every 90 days. (~~TS//SI//NF~~)

[252] As noted above, seed [redacted] are e-mail addresses or telephone numbers for which a reasonable articulable suspicion exists to believe the [redacted] is related to a terrorist entity. Seed [redacted] are used to query the meta data database to reveal links with other addresses or numbers. (~~TS//SI//NF~~)



[redacted] b1, b3, b7E

D. Subsequent PR/TT Applications and Orders ~~(TS//SI//NF)~~

As described above, the PR/TT Order was first renewed on [redacted] and was renewed by subsequent orders of the FISA Court at approximately 90-day intervals.[254] ~~(TS//SI//NF)~~

On [redacted] the FISA Court issued a Supplemental Order requiring the government to enhance its reporting to the Court of the foreign intelligence benefits realized under the PR/TT Orders. Writing for the FISA Court, Judge Kollar-Kotelly stated that the authority granted under these orders allowed the NSA "to collect vast amounts of information about e-mail [redacted] communications[,]" but that "the Court is unable on the current record to ascertain the extent to which information so collected has actually resulted in the foreign intelligence benefits originally anticipated." Supplemental Order at 1-2. The government responded with a motion requesting that, in light of prior briefings it had given the FISA Court, it not be required to fully comply with the Supplemental Order. It is not clear what if any specific action the FISA Court took in response to this motion, although based on the OIG's review of the PR/TT docket the government continued to submit regular reports to the FISA Court.
~~(TS//STLW//SI//OC/NF)~~

Under the PR/TT renewal applications the scope of authorized queries against the PR/TT database remained limited to queries that concerned [redacted] b1, b3, b7E

[redacted]

[254] In these renewals, [redacted] were added and dropped from [redacted] that were approved in the July 14, 2004, PR/TT Order. ~~(TS//SI//NF)~~

[redacted] (TS//SI//NF) b1, b3, b7E

[redacted] b1, b3, b7E

[redacted] b1, b3, b7E

Although the FISA Court continued to renew the NSA's authority to collect and query e-mail meta data, and the NSA proceeded under that authority [redacted] (TS//STLW//SI//OC/NF)

II. Telephony Meta Data Collection Under FISA (TS//SI//NF)

The second part of the Stellar Wind program brought under FISA authority was the NSA's bulk collection of telephony meta data (basket 2). As described in Chapter Three, under this aspect of the Stellar Wind program the NSA obtained the call detail records of telephone calls, domestic and international [redacted] As with e-mail meta data, the bulk

[redacted] b1, b3, b7E

[257] As discussed in Chapter Three, [redacted] Call detail records consist of routing information, including the originating and terminating telephone number of each call, and the date, time, and duration of each call. The call detail records do not include the substantive content of any communication or the name, address, or financial information of a subscriber or customer. (TS//SI//NF)

nature of the telephony collection provided the NSA the ability to conduct [redacted] – contact chaining [redacted] ~~(TS//STLW//SI//OC/NF)~~

The transition of bulk telephony meta data collection from Presidential Authorization under the Stellar Wind program to FISA authority relied on a provision in the FISA statute that authorized the FBI to seek an order from the FISA Court compelling the production of "any tangible things" from any business, organization, or entity, provided the items are for an authorized investigation to protect against international terrorism or clandestine intelligence activities. See 50 U.S.C. § 1861. Orders under this provision commonly are referred to as "Section 215" orders in reference to Section 215 of the USA PATRIOT ACT, which amended the "business records" provision in title V of FISA.[258] The "tangible things" the government sought in the Section 215 application described in this section were the call detail records [redacted] .. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

We describe below the circumstances that led to the government's decision to transition the bulk collection of telephony meta data from presidential authority to FISA Authority. We then summarize the government's initial application and the related Court Order. ~~(TS//STLW//SI//OC/NF)~~

A. Decision to Seek Order Compelling Production of Call detail records ~~(TS//SI//NF)~~

The timing of the Department's decision in May 2006 to seek a FISA Court order for the bulk collection of telephony meta data was driven primarily by external events. On December 16, 2005, The New York Times published an article entitled, "Bush Lets U.S. Spy on Callers Without Courts." The article, which we discuss in more detail in Chapter Eight, described in broad terms the content collection aspect of the Stellar Wind program, stating that the NSA had "monitored the international telephone calls of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible 'dirty numbers' linked to al Qaeda." [redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

258 The term "USA PATRIOT Act" is an acronym for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). It is commonly referred to as "the Patriot Act." (U)

On December 17, 2005, in response to the article, President Bush publicly confirmed that he had authorized the NSA to intercept the international communications of people with "known links" to al Qaeda and related terrorist organizations (basket 1). On January 19, 2006, the Justice Department issued a document entitled "Legal Authorities Supporting the Activities of the National Security Agency Described by the President" and informally referred to as a "White Paper," that addressed in an unclassified form the legal basis for the collection activities that were described in the New York Times article and confirmed by the President.
~~(TS//STLW//SI//OC/NF)~~

According to Steven Bradbury, the head of OLC at that time, the legal analysis contained in the White Paper [redacted] Although the New York Times article did not describe this aspect of Stellar Wind, reporters at USA Today were asking about this aspect of the program in early 2006. Bradbury [redacted] anticipated that a USA Today story would attract significant public attention when it was published.[259] ~~(TS//STLW//SI//OC/NF)~~

[redacted] b1, b3, b7E

[259] On May 11, 2006, USA Today published the results of its investigation. The article, entitled "NSA Has Massive Database of American Phone Calls," reported that the NSA "had been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon, and BellSouth." The article stated that the program, launched shortly after the September 11 attacks, collected the records of billions of domestic calls in order to analyze calling patterns to detect terrorist activity. The article reported that the records provided to the NSA did not include customer names, street addresses, and other personal information, but noted that such information was readily available by cross-checking the telephone numbers against other databases.

~~(TS//STLW//H//OC/NF)~~

[redacted] b1, b3, b7E

[redacted]

B. Summary of Department's Application and Related FISA Court Order ~~(S/NF)~~

As noted previously, applications to the FISA Court that seek an order compelling the production of "tangible things" are commonly referred to as "Section 215" applications, in reference to Section 215 of the USA PATRIOT ACT. Section 215 authorizes the FBI to request a FISA Court order

> requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution. (U)

50 U.S.C. § 1861(a)(1).[261] Section 215 does not require that the items sought pertain to the subject of an investigation; the government need only demonstrate that the items are relevant to an authorized investigation.[262] (U)

On May 23, 2006, the FBI filed with the FISA Court a Section 215 application seeking authority to collect telephony meta data to assist the NSA in finding and identifying known and unknown members or agents of [redacted] in support of the [redacted] related FBI investigations then pending and other Intelligence Community operations. The application requested an order compelling [redacted] to produce (for the duration of the 90-day order) call detail records relating to all telephone communications maintained by the carriers. The application described call detail records as routing information that included the

b1, b3, b7E

---

[261] "United States person" is defined in FISA as a citizen, legal permanent resident, or unincorporated association in which a "substantial number" of members are citizens or legal permanent residents, and corporations incorporated in the United States as long as such associations or corporations are not themselves "foreign powers." 50 U.S.C. § 1801(i)(2005). (U)

[262] Prior to the enactment of Section 215, the FISA statute's "business records" provisions were limited to obtaining information about a specific person or entity under investigation. Also, information could be obtained only from common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities. (U)

originating and terminating telephone number of each call, and the date, time, and duration of each call. The application stated that telephony meta data did not include the substantive content of any communication or the name, address, or financial information of a subscriber or customer. According to the application, the majority of the telephony meta data provided to the NSA was expected to involve communications that were (1) between the United States and abroad, or (2) wholly within the United States, including local telephone calls. [redacted].[263] ~~(TS//SI//NF)~~

The application acknowledged that the [redacted] collection would include records of communications of U.S. persons located within the United States who were not the subject of any FBI investigation. However, relying on the precedent established by the PR/TT Order, the application asserted that the collection was needed for the NSA to perform analysis to find known [redacted] and to identify unknown operatives, some of whom may be in the United States or in communication with U.S. persons. The application stated that it was not possible to determine in advance which particular piece of meta data will identify a terrorist. The application stated that obtaining such bulk data increases the NSA's ability, through contact-chaining [redacted] to detect and identify members of [redacted].[264] In other words, according to the application, meta data analysis is possible only if the NSA "has collected and archived a broad set of metadata that contains within it the subset of communications that can later be identified as terrorist-related."[265] ~~(TS//SI//NF)~~

---

[263] The NSA told us that the actual average amount of telephony meta data collected per day is approximately [redacted] call detail records and that the figure has not reached [redacted] ~~(TS//SI//NF)~~

[264] [redacted] b1, b3, b7E

[265] The FISA Court had stated in its July 2004 PR/TT Order that the FISA statute's "relevance" requirement is a relatively low standard and that in evaluating whether bulk meta data is "relevant" to an investigation into [redacted] "deference should be given to the fully considered judgment of the executive branch in assessing and responding to national security threats and in determining the potential significance of intelligence-related information." The government cited this precedent in the Section 215 application, stating, "[j]ust as the bulk collection of e-mail meta data was relevant to FBI investigations into [redacted] so is the bulk collection of telephony metadata described herein." ~~(TS//SI//NF)~~

The application also explained how the meta data would be used [redacted] [266] The database could be queried only if the NSA determined that, "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [redacted] the Section 215 application, like the PR/TT application and Order, added the following proviso to the query standard: "provided, however, that a telephone number believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution." ~~(TS//SI//NF)~~

According to the application, the NSA estimated that only a tiny fraction (1 in 4 million, or 0.000025 percent) of the call detail records included in the database were expected to be analyzed. The results of any such analysis would be provided, or "tipped," to the FBI or other federal agencies (as was being done under Stellar Wind). [redacted] ~~(TS//SI//NF)~~

The application also proposed restrictions on access to, and the processing and dissemination of, the data collected that were essentially identical to those included in the PR/TT Order. These included the requirement that queries be approved by one of seven NSA officials or managers and that the NSA's Office of the General Counsel would review and approve proposed queries of telephone numbers reasonably believed to be used by U.S. persons.[267] ~~(TS//SI//NF)~~

[266] [redacted]

[267] The application included several other measures to provide oversight of the use of meta data, such as controls on the dissemination of any U.S. person information, the creation of a capability to audit NSA analysts with access to the meta data, the destruction of collected meta data after a period of 5 years (the destruction period for e-mail meta data was 4½ years), and a review by the NSA's Inspector General and General Counsel conducted within 45 days of implementing the FISA Court order that assessed the

(Cont'd.)

On May 24, 2006, the FISA Court approved the Section 215 application. The Court's Order stated that there were reasonable grounds to believe that the telephony meta data records sought were relevant to authorized investigations being conducted by the FBI to protect against international terrorism. The Order incorporated each of the procedures proposed in the government's application relating to access to and use of the meta data. These procedures included a requirement that any application to renew or reinstate the authority for the bulk collection contain a report describing (1) the queries made since the Order was granted; (2) the manner in which the procedures relating to access and use of the meta data were applied; and (3) any proposed changes in the way in which the call detail records would be received from the communications carriers. The Order also requires the Justice Department to review, at least every 90 days, a sample of the NSA's justifications for querying the call detail records. ~~(TS//SI//NF)~~

Through March 2009, the FISA Court renewed the authorities granted in the May 24 Order at approximately 90-day intervals, with some modifications sought by the government. For example, the Court granted a motion filed on August 8, 2006, requesting [redacted][268] [redacted] b1, b3, b7E Except for these and other minor modifications, the terms of the FISA Court's grant of Section 215 authority for the bulk collection of telephony meta data remained essentially unchanged since first approved on May 24, 2006, through March 2009. [redacted] Further, the FISA Court's Section 215 Orders did not require the NSA to modify its use of the telephony meta data from an analytical perspective. However, as discussed below, the FISA Court drastically changed the authority contained in its March 2009 Section 215 Order following the government's disclosure of incidents involving the NSA's failure to comply with the terms of the Court's prior orders. ~~(TS//STLW//SI//OC/NF)~~

---

adequacy of the management controls for the processing and dissemination of U.S. person information. ~~(TS//SI//NF)~~

[268] As noted above, the Court granted an identical motion at the same time in connection with the bulk collection of e-mail meta data. ~~(TS//SI//NF)~~

C. Non-Compliance with Section 215 Orders ~~(TS//SI//NF)~~

On January 9, 2009, representatives from the Department's National Security Division attended a briefing at the NSA concerning the telephony meta data collection. During the course of this briefing, and as confirmed by the NSA in the days that followed, the Department came to understand that the NSA was querying the telephony meta data in a manner that was not authorized by the FISA Court's Section 215 Orders. Specifically, the NSA was on a daily basis automatically querying the meta data with thousands of telephone identifiers from an "alert list" that had not been determined to satisfy the reasonable articulable suspicion (RAS) standard the Court required be met before the NSA was authorized to "access the archived data" for search or analysis purposes.[269] ~~(TS//SI//NF)~~

The alert list contained telephone identifiers that were of interest to NSA counterterrorism analysts responsible for tracking the targets of the Section 215 Orders [redacted] The list was used to compare the incoming telephony meta data obtained under FISA authority. [redacted] Under the procedures the NSA had developed to implement the Section 215 authority, alerts (or matches) generated from RAS-approved identifiers could be used to automatically conduct contact chaining [redacted] of the telephony meta data. However, automated analysis for alerts generated by non-RAS approved identifiers were not permitted; instead, the alerts were sent to analysts to determine whether chaining [redacted] was warranted in accordance with the RAS standard. ~~(TS//SI//NF)~~ b1, b3, b7E

On January 15, 2009, the Justice Department notified the FISA Court that the NSA had been accessing the telephony meta data with non-RAS approved identifiers. [redacted].[270] On January 28, 2009, the b1, b3, b7E

[269] The term "telephone identifier" used by the government means a telephone number as well as other unique identifiers associated with a particular user or telecommunications device for purposes of billing or routing communications. ~~(TS//SI//NF)~~

[270] Following the Department's notice to the Court, the NSA attempted to complete a software fix to the alert process so that "hits" against the telephony meta data generated by non-RAS-approved telephone identifiers were deleted and that only "hits" generated by RAS-approved identifiers were sent to NSA analysts for further analysis. The NSA also attempted to construct a new alert list consisting of only RAS-approved telephone identifiers. However, the implementation of these modifications was unsuccessful and on January 24, 2009, the NSA shut down the alert process completely. ~~(TS//SI//NF)~~

Court issued an order stating that it was "exceptionally concerned about what appears to be a flagrant violation of its Order in this matter[.]" The Court required the government to file a brief to "help the Court assess whether the Orders in this docket should be modified or rescinded; whether other remedial steps should be directed; and whether the Court should take action regarding persons responsible for any misrepresentations to the Court or violation of its Orders, either through its contempt powers or by referral to appropriate investigative offices." The Court also required the government to address several additional specific issues, including who knew that the alert list being used to query the meta data included identifiers that had not been determined to meet the reasonable and articulable suspicion standard, how long the "unauthorized querying" had been conducted, and why none of the entities the Court directed to conduct reviews of the meta data collection program identified the problem earlier.[271] ~~(TS//SI//NF)~~

On February 17, 2009, the government responded to the Court's Order and acknowledged that the NSA's previous descriptions to the Court of the alert list process were inaccurate and that the Section 215 Order did not authorize the government to use the alert list in the manner that it did. The government described for the Court in detail how the NSA developed procedures in May 2006 to implement the Section 215 authority that resulted in the NSA querying the telephony meta data with non-RAS approved telephone identifiers for over 2 years in violation of the Court's Orders, and how those procedures came to be described incorrectly to the Court. According to the government, the situation resulted from the NSA's interpretation of the term "archived data" used in the Court's Orders and the NSA's mistaken belief that the alert process under the Section 215 authority operated the same as the alert process under the Pen Register/Trap and Trace authority.[272] The government told the Court that "there was never a complete understanding among key personnel" who reviewed the initial report to the Court describing the alert process about

---

[271] The entities directed to conduct such reviews under the Section 215 Orders were the NSA's Inspector General, General Counsel, and Signals Intelligence Directorate Oversight and Compliance Office. (U//~~FOUO~~)

[272] The NSA understood the term "archived data" in the Court's Order to refer to the NSA's analytical repository for the telephony meta data. As the term is normally used by [redacted] The NSA believed that the requirement to satisfy the RAS standard was only triggered when the NSA sought access to the stored, or "archived," repository of telephony meta data. For this reason, in the NSA's view, it was not required to limit the alert list to RAS-approved identifiers. ~~(TS//SI//NF)~~

what certain terminology was intended to mean, and that "there was no single person who had complete technical understanding of the BR FISA system architecture." ~~(TS//SI//NF)~~

The government argued that the Section 215 Orders should not be rescinded or modified "in light of the significant steps that the Government has already taken to remedy the alert list compliance incident and its effects, the significant oversight modifications the Government is in the process of implementing, and the value of the telephony metadata collection to the Government's national security mission[.]"[273] Among the several measures the government highlighted to the Court was the NSA Director's decision to order "end-to-end system engineering and process reviews (technical and operational) of NSA's handling of [telephony] metadata." Less than two weeks after the government filed the response summarized above, the government informed the Court that the NSA had identified additional compliance incidents during these reviews.[274] ~~(TS//SI//NF)~~

In Orders dated March 2 and 5, 2009, the FISA Court addressed the compliance incidents reported by the government and imposed drastic changes to the Section 215 authorities previously granted. The Court first addressed the NSA's interpretation of the term "archived data." The Court said the interpretation "strains credulity" and observed that an interpretation that turns on whether the meta data being accessed has been "archived" in a particular database at the time of the access would "render compliance with the RAS requirement merely optional." ~~(TS//SI//NF)~~

[273] [redacted] The NSA also determined that in all instances that a U.S. telephone identifier was used to query the meta data for a report, the identifier was either already the subject of a FISA Court order or had been reviewed by the NSA's Office of General Counsel to ensure the RAS determination was not based solely on a U.S. person's First Amendment-protected activities. ~~(TS//SI//NF)~~

[274] The additional compliance incidents involved the NSA's handling of the telephony meta data in an unauthorized manner. The first incident involved the NSA's use of an analytical tool to query (usually automatically) the meta data with non-RAS approved telephone identifiers. The tool determined if a record of a telephone identifier was present in NSA databases and, if so, provided analysts with information about the calling activity associated with that identifier. The second incident involved three analysts who conducted chaining analyses in the telephony meta data using 14 non-RAS approved identifiers. According to the government's notice to the Court, the analysts conducted queries of non-FISA authorized telephony meta data and were unaware their queries also ran against the FISA-authorized meta data. The government stated that none of the queries used an identifier associated with a U.S. person or telephone identifier and none of the queries resulted in intelligence reporting. ~~(TS//SI//NF)~~

The Court next addressed the misrepresentations the government made to the Court from August 2006 to December 2008 in reports that inaccurately described the alert list process. The Court recounted the specific misrepresentations and summarized the government's explanation for their occurrence. The Court then concluded,

> Regardless of what factors contributed to making these misrepresentations, the Court finds that the government's failure to ensure that responsible officials adequately understood the NSA's alert list process, and to accurately report its implementation to the Court, has prevented, for more than two years, both the government and the FISC from taking steps to remedy daily violations of the minimization procedures set forth in FISC orders and designed to protect [redacted] call detail records pertaining to telephone communications of U.S. persons located within the United States who are not the subject of any FBI investigations and whose call detail information could not otherwise have been legally captured in bulk. ~~(TS//SI//NF)~~

The Court also addressed the additional non-compliance incidents that were identified during the initial review ordered by the NSA Director, observing that the incidents occurred despite the NSA implementing measures specifically intended to prevent their occurrence. In view of the record of compliance incidents the government had reported to date, the Court stated,

> [I]t has finally come to light that the FISC's authorizations of this vast collection program have been premised on a flawed depiction of how the NSA uses BR metadata. This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively. ~~(TS//SI//NF)~~

Despite the Court's concerns with the telephony meta data program, and its lack of confidence "that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders," it authorized the government to continue collecting telephony meta data under the Section 215 Orders. The Court explained that in light of the

government's repeated representations that the collection of the telephony meta data is vital to national security, taken together with the Court's prior determination that the collection properly administered conforms with the FISA statute, "it would not be prudent" to order the government to cease the bulk collection. ~~(TS//SI//NF)~~

However, believing that "more is needed to protect the privacy of U.S. person information acquired and retained" pursuant to the Section 215 Orders, the Court prohibited the government from accessing the meta data collected "until such time as the government is able to restore the Court's confidence that the government can and will comply with previously approved procedures for accessing such data."[275] The government may, on a case-by-case basis, request authority from the Court to query the meta data to obtain foreign intelligence.[276] Such a request must specify the telephone identifier to be used and the factual basis for the NSA's RAS determination. ~~(TS//SI//NF)~~

The Court ordered that upon completion of the NSA's end-to-end system engineering and process reviews, the government file a report that describes the results of reviews, discusses the steps taken to remedy non-compliance incidents, and proposes minimization and oversight procedures to employ should the Court authorize resumption of regular access to the telephony meta data. The government's report also must include an affidavit from the FBI Director and any other government national security official deemed appropriate describing the value of the telephony meta data to U.S. national security. ~~(TS//SI//NF)~~

Additionally, the Court ordered the government to implement oversight mechanisms proposed in the government's response to the compliance incidents. These mechanisms generally require the Justice Department's National Security Division to assume a more prominent role in the NSA's administration of the bulk collection program. For example, the NSA's Office of General Counsel must now consult with the National

---

[275] The Court also stated, "Given the Executive Branch's responsibility for and expertise in determining how best to protect our national security, and in light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified, in the view of those responsible for our national security, and that it is being implemented in a manner that protects the privacy interests of U.S. persons[.]" ~~(TS//SI//NF)~~

[276] The Court authorized the government to query the meta data without Court approval to protect against an imminent threat to human life, with notice to the Court within the next business day of the query being conducted. The Court also authorized the government to access the meta data to ensure "data integrity" and to develop and test technological measures designed to enable to the NSA to comply with previously approved procedures for accessing the meta data. ~~(TS//SI//NF)~~

Security Division on all significant legal opinions that relate to the interpretation, scope, or implementation of past, current, and future Section 215 Orders related to the telephony bulk meta data collection. ~~(TS//SI//NF)~~

On May 29, 2009, the Court authorized the government to continue collecting telephony meta data under the Section 215 Orders for 43 days subject to the same limitations set out in its orders of March 2 and 5, 2009. ~~(TS//SI//NF)~~

III. Content Collection under FISA ~~(TS//SI//NF)~~

The third and last part of the Stellar Wind program brought under FISA authority was content collection (basket 1). The effort to accomplish this transition was legally and operationally complex, and our discussion in this section does not address each statutory element or the full chronology of the government's applications and related FISA Court orders. Rather, we describe the circumstances surrounding the government's decision to transition content collection from presidential to FISA authority [redacted] We also summarize the FISA Court's response to the government's content collection proposals and the orders it issued. In this section, we describe one FISA Court judge's rejection of the government's legal approach to content collection, a decision that hastened the enactment of legislation that significantly amended the FISA statute and provided the government surveillance authorities broader than those authorized under Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

A. Decision to Seek Content Order ~~(TS//SI//NF)~~

The Department first began work on bringing Stellar Wind's content collection activity (basket 1) under FISA in March 2005, shortly after Alberto Gonzales became Attorney General. Gonzales told us that he initiated discussions about making this change with OLC Principal Deputy Assistant Attorney General Bradbury. Gonzales said that he had questions about how the NSA was conducting the collection in terms of audits and checks being performed, and he wanted to ensure that the agency was running the program properly. Gonzales told us that placing content collection under FISA authority would also eliminate the constitutional debate about the activity and would reassure people that the President was acting according to the Constitution and the law. Gonzales said that, in his view, it is better to conduct activities such as content collection without a direct order from the President when possible. Gonzales added that in 2001 nobody thought it was possible to bring Stellar Wind under FISA authority. ~~(TS//STLW//SI//OC/NF)~~

When Gonzales became Attorney General in early 2005, however, he also knew there had been a leak to The New York Times about the NSA's content collection activity under Stellar Wind and that the paper was actively investigating the story. In November 2004, Gonzales (then the White House Counsel), together with Deputy Attorney General Comey and his Chief of Staff, had met with New York Times reporters to discuss the potential article.[277] ~~(TS//STLW//SI//OC/NF)~~

In response to Gonzales's request, Bradbury, working with attorneys in OLC and the Office of Intelligence and Policy Review (OIPR) as well as with NSA personnel, devised a legal theory, summarized below, for bringing under FISA the Stellar Wind program's content collection activities while preserving the "speed and agility" many Intelligence Community officials cited as the chief advantage of the NSA program. In June 2005, Bradbury, together with Associate Deputy Attorney General Patrick Philbin, presented the legal theory to White House officials David Addington, Harriet Miers, and Daniel Levin and received their approval to continue work on a draft FISA application.[278] ~~(TS//STLW//SI//OC/NF)~~

Bradbury told the OIG that he also spoke to the Director of National Intelligence and to NSA officials about bringing Stellar Wind's content collection under FISA. According to Bradbury, the Director of National Intelligence responded positively to the proposal, but the NSA was skeptical as to whether a FISA approach would be feasible, in view of the substantial administrative requirements under the FISA Court's PR/TT Order. The NSA also believed that the FISA Court would be reluctant to grant the NSA the operational flexibility it would insist on in any content application, resulting in less surveillance coverage of telephone numbers and e-mail addresses used by persons outside the United States. ~~(TS//STLW//SI//OC/NF)~~

As discussed in detail in Chapter Eight of this report, in December 2005 The New York Times published its series of articles on the content collection portion of the Stellar Wind program, resulting in considerable controversy and public criticism of the NSA program. Through the spring of 2006, the Department continued work on the content application. In May 2006, at the first of the FISA Court's semiannual meetings that year, the Department provided the Court a draft of the application for content collection to obtain feedback on the government's unconventional approach to the FISA statute. None of FISA Court judges indicated whether the

---

[277] The New York Times held the article until December 2005, when it published a series of articles on the content collection portion of Stellar Wind. ~~(TS//SI//NF)~~

[278] After serving as Acting Assistant Attorney General for OLC from June 2004 to February 2005, Levin joined the National Security Council, where he remained until approximately November 2005. (U)

application would be granted if filed, but some identified concerns with certain aspects of the proposal. ~~(TS//STLW//SI//OC/NF)~~

At this time, Congress and the Administration were also discussing how to modernize the FISA statute to authorize the type of electronic surveillance that the content application sought. Work on the application was temporarily suspended as the Department focused its attention on working with Congress to craft this legislation. However, this suspension of work on the content application was brief. Bradbury said he concluded by the fall of 2006, as Congress was heading for recess, that there would be no legislative reform of the FISA statute in the foreseeable future that would address content collection as it was being conducted under Stellar Wind. As a result, the Department pressed forward with the draft content application to the FISA Court. ~~(TS//STLW//SI//OC/NF)~~

B. Summary of Department's December 13, 2006, Content Application ~~(TS//SI//NF)~~

In November 2006, at the second of the Court's semiannual meetings, the Department presented an updated draft of the application that incorporated feedback received from members of the Court during the previous semiannual meeting. On December 13, 2006, the Department formally filed the content application with the Court. ~~(TS//SI//NF)~~

The government's December 13 application sought authority to intercept the content of telephonic and electronic communications of [redacted] [redacted][279] The application stated: b1, b3, b7E

> Speed and flexibility are essential in tracking individuals who [redacted] To follow the trails effectively, and to respond to new leads, it is vital for the U.S. Intelligence Community to be able quickly and efficiently to acquire communications to or from individuals reasonably believed to

[279] The content application included the following caveat:

By filing this application, the United States does not in any way suggest that the President lacks constitutional or statutory authority to conduct the electronic surveillance detailed herein without Court authorization. ~~(TS//SI//NF)~~

be members or agents of these [redacted] foreign powers. ~~(TS//SI//NF)~~

According to the application, the goal was to establish "an early warning system" under FISA to alert the government to the presence of members and agents of foreign powers [redacted] and to assist tracking such individuals within the United States. The "early warning system" sought to replace the conventional practice under FISA of filing individual applications each time the government had probable cause to believe that a particular phone number or e-mail address, referred to by the NSA as a "selector," was being used or about to be used by members or agents of a foreign power. ~~(TS//SI//NF)~~ b1, b3, b7E

In the place of this individualized process, the application proposed that the FISA Court establish broad parameters for the interception of communications – specifically, [redacted] that can be targeted and the locations where the surveillance can be conducted – and that NSA officials, rather than FISA Court judges, determine within these parameters the particular selectors whose communications the NSA would intercept. [redacted] albeit with FISA Court review and supervision.[280] ~~(TS//SI//NF)~~

The legal arguments underlying the government's approach are complex and involve substantial communications terminology. They also require lengthy discussion of the FISA statute and previous FISA Court decisions. Rather than describe at length these issues, in this section we detail the two main components of the government's approach to content collection in the FISA application that are critical for understanding one judge's approval of the application and another judge's later rejection of essentially the same application. ~~(TS//SI//NF)~~

First, the government proposed an interpretation of the term "facility" in the FISA statute that was broader than how the term was ordinarily, but

---

[280] The Department's application provided an example to illustrate the risks associated with the existing requirement that FISA Court approval or Attorney General emergency authorization be obtained each time the government seeks to target a particular telephone number or e-mail address: [redacted] According to the application, valuable intelligence could be lost in the time it would take to receive FISA Court authorization or Attorney General emergency authorization to target the new address. ~~(TS//SI//NF)~~

not always, applied.[281] Section 1805(a)(3)(B) of FISA provides that the Court may order electronic surveillance only upon finding that there is probable cause to believe that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by" a group involved in international terrorism. The term "facilities" generally was interpreted to refer to individual telephone numbers or e-mail addresses at which surveillance is "directed." ~~(TS//SI//NF)~~

The government proposed in its content application that the term "facilities" be interpreted broadly to include [redacted].[282] Under this approach, instead of examining the target's use of particular telephone numbers or e-mail addresses, the Court would determine only whether there was probable cause to believe that the target was using [redacted] to communicate telephonically or by e-mail.[283] ~~(TS//STLW//SI//OC/NF)~~

Second, the government's application requested that senior NSA officials be authorized to make individualized findings of probable cause about whether a particular telephone number or e-mail address was being used by a member or agent of one of the application's targets. Ordinarily, a FISA Court judge makes this probable cause determination. ~~(TS//SI//NF)~~

To implement this transfer of authority, the government proposed that NSA officials make the probable cause determinations as part of requirements called "minimization procedures," which are detailed rules

---

[281] The government's Memorandum of Law filed in support of the content application described several instances where the FISA Court authorized surveillance of facilities that was not limited to particular telephone numbers and e-mail addresses. According to the application, [redacted] The government's proposed interpretation of the term in the content application was far broader than previously authorized by the Court. ~~(TS//SI//NF)~~

[282] [redacted] b1, b3, b7E

[283] As noted, the targets of the content application were [redacted] The government's content application included a declaration from the NSA Director that addressed [redacted] use of the international telephone system and [redacted] communications. ~~(TS//SI//NF)~~ b1, b3, b7E

that govern how the government must handle communications that it intercepts pertaining to U.S. persons. The FISA statute provides that each FISA application must include, and the FISA Court must approve, minimization procedures that the agency will follow with respect to communications intercepted pursuant to a FISA Court order. ~~(TS//SI//NF)~~

Minimization procedures, in the FISA context, ordinarily govern the handling of intercepted communications involving U.S. persons after the acquisition has been approved by the FISA Court. In other words, a FISA Court authorizes the agency to intercept the communications of particular selectors, and the agency follows the minimization procedures with respect to how it retains, uses, and disseminates any U.S. person information it collects under the Court's order. ~~(TS//SI//NF)~~

However, the government proposed as part of the content application that the minimization procedures also encompass how the NSA acquires the communications.[284] Specifically, the application proposed that the NSA could intercept the communications of specific selectors if agency officials determined there was probable cause to believe that (1) the selector is being used by a member or agent of a [redacted] and (2) the communication is to or from a foreign country. The application referred to this as the "minimization probable cause standard."[285] ~~(TS//SI//NF)~~ b1, b3, b7E

Thus, the content application had a two-prong "minimization probable cause standard": (1) probable cause to believe a selector is being used by a member or agent of a targeted group, and (2) probable cause to believe the communication intercepted is to or from a foreign country. [redacted]

---

[284] Bradbury told the OIG that this argument was based on the text of the FISA statute, which states that minimization procedures apply to the "acquisition" of communications in addition to their retention and dissemination. See 50 U.S.C. § 1801(h)(1). Indeed, the government's Memorandum of Law filed in support of the content application described several cases in which the FISA Court authorized the government to conduct electronic surveillance that included minimization at the time of acquisition. According to the application, the cases involved surveillance broadly targeted [redacted] than those the government specifically sought to acquire. [redacted] ~~(TS//SI//NF)~~ b1, b3, b7E

[285] The proposed "minimization probable cause standard" was in addition to the standard minimization procedures that accompany every FISA application submitted by the government and that have been long-approved by the FISA Court. ~~(TS//SI//NF)~~

[redacted] (~~TS//STLW//SI//OC/NF~~)

For the first prong – probable cause to believe a selector is being used by a member or agent of a targeted group – NSA analysts would assess sources of "reliable intelligence," defined in the application as information from a variety of domestic and foreign intelligence and law enforcement activities. Under the terms of the application, positive findings of probable cause would be recorded in a database and the assessment process would be subject to periodic internal review by NSA officials, including the NSA General Counsel and Inspector General. (~~TS//SI//NF~~)

For the second prong – probable cause to believe the communication intercepted is to or from a foreign country [redacted] For example, the application stated that there would be probable cause to believe [redacted] b1, b3, b7E

[redacted][286] With respect to e-mails, the application stated that [redacted] [287] (~~TS//STLW//SI//OC/NF~~)

---

[286] The application acknowledged that communications intercepted at the "facilities" could include some calls where [redacted] in the United States, or where [redacted] in the United States (even where there is probable cause to believe that [redacted] the United States). [redacted] b1, b3, b7E

[redacted] If the NSA had probable cause to believe one of the communicants was a member of [redacted] the call could be intercepted. The application stated that such communications would be handled in accordance with NSA's standard minimization procedures that apply to all of the agency's electronic surveillance activities. (~~TS//SI//NF~~)

[287] As it did with telephone communications, the application acknowledged that the manner in which e-mail communications are routed would cause the NSA to collect some e-mail communications that in fact are between communicants wholly within the United (Cont'd.)

Thus, viewing the government's approach to both "facilities" and "minimization procedures" together, the December 13, 2006, content application asked the FISA Court to find probable cause to believe that [redacted] engaged in international terrorism, and that these groups use the international telephone system and the [redacted] communications system [redacted] Then, within these broad parameters authorized by the Court, NSA officials would make probable cause findings about whether individual telephone numbers or e-mail addresses are used by members or agents of [redacted] and whether the communications of those numbers and addresses are to or from a foreign country. If they were, the NSA could direct the telecommunications carriers to intercept the communications of those telephone numbers and e-mail addresses and provide them to the NSA. [redacted] (~~TS//STLW//SI//OC/NF~~) b1, b3, b7E

Under the terms of the application, communications acquired by the NSA could be retained for 5 years, unless the Court approved retention for a longer period. The application also stated that the NSA expected to initially target [redacted] telephone numbers and e-mail addresses used by members or agents of [redacted] (~~TS//SI//NF~~) b1, b3, b7E

An additional aspect of the content application is important to understand. The "early warning system" the government proposed applied both to "domestic selectors" and "foreign selectors." Domestic selectors are telephone numbers and e-mail addresses reasonably believed to be used by individuals in the United States; foreign selectors are telephone numbers and e-mail addresses reasonably believed to be used by individuals outside the United States. Under Stellar Wind, the NSA intercepted the communications of both categories of selectors, although the NSA tasked far more foreign selectors than domestic selectors. ~~(TS//STLW//SI//OC/NF)~~

States, even though the NSA had probable cause to believe the communication was to or from a foreign country. The application stated that the NSA would handle any such communications in accordance with its standard minimization procedures. ~~(TS//SI//NF)~~

The government proposed in its content application that the domestic selectors would be subject to more rigorous targeting approval and more frequent reporting to the FISA Court than foreign selectors, but the application sought to preserve NSA officials' authority to make the probable cause determinations as to each.[288] As we describe below, the first FISA Court judge to consider the content application, Judge Malcolm Howard, was unwilling to extend this authority to domestic selectors. ~~(TS//SI//NF)~~

C. Judge Howard Grants Application in Part ~~(TS//SI//NF)~~

The Department's December 13, 2006, content application was assigned to Judge Howard, because he was the "duty" judge that week responsible for considering new applications.[289] Judge Howard advised the Department orally that he would not authorize, on the terms proposed in the application, the electronic surveillance of selectors to be used by persons in the United States (domestic selectors). He did not issue a written opinion or order concerning this decision. The Department, in response to Judge Howard's oral advisement, filed a separate application requesting authority to conduct electronic surveillance on domestic selectors. This application, summarized below, was filed on January 9, 2007, and is considered the first "domestic selectors application"; the December 13 application is considered the first "foreign selectors application." ~~(TS//SI//NF)~~

Judge Howard also requested additional briefing from the Justice Department on the subject of whether [redacted] constituted "facilities" under FISA, and whether the surveillance authority sought in the government's content application would in fact be "directed" not at these "facilities" but rather at the particular telephone numbers and e-mail addresses the government would task for collection. ~~(TS//SI//NF)~~ b1, b3, b7E

In response, the Department filed a supplemental memorandum of law on January 2, 2007, arguing that the government's construction of the

---

[288] Under the terms of the original content application, domestic selectors tasked by the government would subsequently be reported to the Court for approval. The Court either had to approve each domestic selector within 48 hours of receiving the government's report or, if the Court did not agree there was probable cause to believe the selector was being used by a member or agent of a target of the application, provide the government 24 hours to submit additional information establishing probable cause. Foreign selectors tasked by the government did not require subsequent approval by the Court, although the Court could direct that the surveillance of any selector cease. ~~(TS//SI//NF)~~

[289] The Department offered to submit the application to the FISA Presiding Judge, Judge Kollar-Kotelly, but she said that it should be filed in the normal fashion, which meant it would be assigned to the FISA duty judge that week. ~~(TS//SI//NF)~~

terms "facilities" and "directed" was fully consistent with the text of FISA and supported by FISA Court practice and precedent. The memorandum further explained why the traditional approach to surveillance under FISA would not provide the speed and agility necessary for the "early warning system" the application sought to create.[290] ~~(TS//SI//NF)~~

On January 10, 2007, Judge Howard approved the Department's content application as to foreign selectors, endorsing the legal framework on which the content application for foreign selectors was based, including the broad construction of the term "facility" and the use of minimization procedures to empower NSA officials to make targeting decisions about particular selectors. Judge Howard's Order authorized the government to conduct electronic surveillance for a period of 90 days at the "facilities" identified in the application, and was set to expire on April 6, 2007. The Order [redacted] b1, b3, b7E [redacted].[291] ~~(TS//SI//NF)~~

Judge Howard's Order also required that an attorney from the Justice Department's National Security Division review the NSA's justifications for targeting particular foreign selectors. The Order required the government to submit reports to the FISA Court every 30 days listing new selectors tasked during the previous 30 days and briefly summarizing the basis for the NSA's determination that the first prong of the minimization probable cause standard has been met for each new selector.[292] The Order preserved the Court's authority to direct that surveillance cease on any selectors for which

---

[290] On this point, the memorandum cited the government's limited resources as presenting a significant obstacle to filing a separate FISA application for each selector it wanted to place under surveillance. The government stated that it anticipated initiating collection on [redacted] new selectors each month, a figure that translates to filing a [redacted] motion to amend a FISA order or seeking Attorney General emergency authority [redacted] times per day (or, alternatively, filing one motion or seeking one Attorney General emergency authorization covering [redacted] new selectors each day). The government stated that if the government proceeded under any of these options, valuable intelligence would be lost. ~~(TS//SI//NF)~~ b1, b3, b7E

[291] As noted earlier, the Order compelled [redacted] The Order also required that with each request for reauthorization, the government present a list of current selectors previously reported to the Court that the government intended to continue tasking, identify any selectors reasonably believed to be used by U.S. persons outside the United States, and assess the efficacy of the collection of communications that mentioned a tasked e-mail address [redacted] but that were not to or from that selector. ~~(TS//SI//NF)~~ b1, b3, b7E

[292] As noted above, the first prong of the standard is probable cause to believe that the selector is being used by a member or agent of a targeted [redacted]. ~~(TS//SI//NF)~~ b1, b3, b7E

the Court found that the first prong of the standard has not been satisfied. In addition, the Order required the NSA Inspector General, General Counsel, and Signals Intelligence Directorate to periodically review the authorized collection activities. These NSA offices were required to submit a report to the Court 60 days after the collection was initiated under the Order that would address the adequacy of management controls and whether U.S. person information was being handled properly. ~~(TS//SI//NF)~~

According to several Department and NSA officials, the effort to implement Judge Howard's January 10, 2007, Order was a massive undertaking. [redacted] b1, b3, b7E ~~(TS//STLW//SI//OC/NF)~~

As a result of the Order, the Department and NSA submitted to the FISA Court for its review the factual basis for each selector supporting the government's determination that the "minimization probable cause standard" had been satisfied. The Department accomplished this pursuant to a schedule approved by Judge Howard under which the Department filed [redacted] foreign selectors every [redacted] days for the duration of the 90-day Order. ~~(TS//SI//NF)~~ b1, b3, b7E

The probable cause explanation for each foreign selector filed with the Court typically was described in several sentences. According to Bradbury, he impressed upon the NSA that Judge Howard would review each submission and inquire about how recently the NSA had acquired communications relating to a particular selector. According to Matthew Olsen, the Deputy Assistant Attorney General in the Department's National Security Division who was responsible for overseeing intelligence matters, Judge Howard did in some cases inquire about the government's factual basis for believing the minimization probable cause standard has been met.[293] Bradbury also said he stressed that the Court would scrutinize the NSA's probable cause determinations more rigorously than the agency had been doing itself and that the Court was more likely to approve a selector where the surveillance was current than it would a selector that has "remained dormant for months."[294] ~~(TS//SI//NF)~~

---

293 Olsen was involved in the drafting and presentation to the FISA Court of the content application and the government's implementation of the related FISA Court Orders. ~~(TS//SI//NF)~~

294 However, Bradbury noted that the FISA Court's "tendency to look for recent information" in assessing whether the probable cause standard has been met is "problematic" because [redacted] (Cont'd.)

Olsen told us that [redacted] foreign selectors ultimately were filed with the FISA Court under the terms of Judge Howard's Order. Olsen said that the NSA strived to submit selectors that were deemed high priority, that had a well-documented nexus to [redacted] foreign powers, and that had recent communications activity. Attorneys from OIPR, who under the terms of the Order were required to review the NSA's justification for each foreign selector that it tasked, worked with the NSA on this large-scale review process. According to Olsen, OIPR attorneys "double-checked" the NSA's probable cause determination for each selector, but did not conduct independent probable cause inquiries. This review identified [redacted] selectors that in OIPR's judgment required additional documentation before they could be submitted to the Court.[295] Olsen described the back-and-forth between OIPR and the NSA as "constant," and said the NSA was receptive to OIPR's involvement. Olsen stated that the NSA committed significant resources to the transition of foreign selectors. ~~(TS//SI//NF)~~ b1, b3, b7E

Both Bradbury and Olsen observed that the transition of content collection of foreign selectors to FISA required some adjustment by the NSA in its approach to establishing probable cause. For example, while an NSA analyst might base a probable cause determination to some extent on intuition, similar to a "cop on the beat," it was a different proposition when that probable cause determination had to be reviewed by several OIPR attorneys trying to anticipate how the FISA Court might view the judgment. Olsen stated that it was also "new" for the NSA to document the probable cause to the level OIPR believed the FISA Court would require. According to Bradbury, the effort sought an equilibrium between "the necessary speed and agility" and the "multiple layers of probable cause determination." Bradbury and Olsen both told the OIG that the NSA had concerns about whether the FISA approach to content collection would work and the extent to which a measure of effectiveness would be lost under FISA Court supervision. ~~(TS//SI//NF)~~

D. Domestic Selectors Application and Order ~~(TS//SI//NF)~~

In contrast to foreign selectors, Judge Howard advised the Justice Department that requests for surveillance of the international calls of domestic selectors – telephone numbers or e-mail addresses reasonably believed to be used by individuals in the United States – should be filed with

[redacted] ~~(TS//SI//NF)~~

[295] Olsen told the OIG that he believes the NSA de-tasked some of these foreign selectors. ~~(TS//SI//NF)~~

the Court in a separate application. Judge Howard also advised OIPR officials that any such application should take a more traditional approach to FISA, meaning the "facilities" targeted by the application should be particular telephone numbers and e-mail addresses and that the probable cause determination for tasking a selector would reside with the FISA Court, not with NSA officials pursuant to minimization procedures. ~~(TS//SI//NF)~~

On January 9, 2007, the Department filed the first domestic selectors application. The application sought two things. First, the application requested authority to intercept the international communications of [redacted] specific domestic selectors.[296] Second, the application sought, for purposes of future applications, approval to use a "streamlined version" of the emergency authorization procedures available under FISA. These emergency procedures authorize the use of electronic surveillance for a period of up to 72 hours without a Court order when the Attorney General reasonably determined that an emergency situation exists. See 50 U.S.C. § 1805(f). The procedures required the Attorney General to inform the FISA Court that the surveillance has been initiated and required the Department to file with the Court an emergency application to continue the surveillance not more that 72 hours after the surveillance was authorized. ~~(TS//SI//NF)~~ b1, b3, b7E

The goal of the Department's proposed streamlined emergency application procedures, referred to in the January 9, 2007, application as a "Verified Application," was to ensure that the emergency surveillance process be completed as swiftly as possible for qualifying domestic selectors. The proposal allowed the Verified Application to incorporate by reference the reasons or facts contained in the original domestic selectors application necessary to satisfy some of the statutory requirements under FISA, instead of reestablishing in each application for a new domestic selector that each of the requirements of FISA were met. The only new substantive information contained in a Verified Application would be the identity of the target, if known, the telephone number the target was using or was about to use, and the factual basis supporting probable cause to believe the target is [redacted] and is using or is about to use the identified telephone number. ~~(TS//SI//NF)~~

Judge Howard granted the domestic selectors application on January 10, 2007, for a period of 90 days. His Order also approved the

---

[296] Unlike the December 13, 2006, application, the January 9, 2007, application did not seek authority to target agents of [redacted] nor did the application seek authority to conduct content surveillance of e-mail communications. The declaration summarized for each of the domestic selectors, generally in two to three paragraphs, the facts that supported the government's belief that the telephone number was used or about to be used by a known or unknown agent of [redacted] located in the United States. (TS//SI//NF) b1, b3, b7E

streamlined emergency authorization procedures proposed in the application for any additional domestic selectors whose communications the government sought to intercept during the 90-day period for which surveillance was authorized.[297] ~~(TS//SI//NF)~~

NSD Deputy Assistant Attorney General Olsen told the OIG that in comparison with foreign selectors, the Department conducted a more rigorous review of the initial domestic selectors submitted to the FISA Court to ensure that probable cause was met. Olsen said a few domestic selector packages "on [their] face" lacked sufficient documentation and that these deficiencies were apparent to OIPR attorneys reviewing the information because the attorneys were looking at the information for the first time. He said that the NSA analysts responsible for the selectors, in contrast, were very familiar with the numbers and knowledgeable of details about the users that might not have been evident to persons reviewing documentation *de novo*. According to Olsen, for selector packages that were considered deficient, the NSA either provided the Justice Department attorneys with additional information or de-tasked the selector.[298] ~~(TS//SI//NF)~~

E. Last Stellar Wind Presidential Authorization Expires ~~(TS//SI//NF)~~

On December 8, 2006, the President signed what would become the final Presidential Authorization for the Stellar Wind program. The December 8 Authorization was scheduled to expire on February 1, 2007. However, Judge Howard's January 10, 2007, Orders relating to foreign and domestic selectors completed the transition of Stellar Wind's

---

[297] On January 22, 2007, the Department filed, and Judge Howard approved, the first Verified Application with the FISA Court using the streamlined procedures approved in the Order. ~~(TS//SI//NF)~~

[298] Olsen and OIPR Deputy Counsel Margaret Skelly-Nolen told the OIG that during the application for and implementation of the domestic selectors Order, it became apparent that there were coordination problems between the FBI and the NSA. They noted that in many instances a domestic selector the NSA sought to task was already targeted by an FBI FISA order. According to Skelly-Nolen, in those cases problems can arise in providing accurate, current, and consistent information to the FISA Court about such selectors. She said the NSA's practice has been to consult with the FBI analysts assigned to the NSA and to request from them the most current information the FBI has about a particular telephone number or user of that number. The FBI analysts at the NSA have access to FBI databases to search for such information, although the most current information frequently can only be obtained from the operational personnel at FBI Headquarters. As a consequence, according to Skelly-Nolen, the FISA Court has on some limited occasions been provided inconsistent information concerning domestic telephone numbers or the users of those numbers. Olsen told the OIG that the domestic selectors Order has required a higher level of coordination between the FBI and NSA and that the National Security Division has worked to address this issue. ~~(TS//SI//NF)~~

communications and meta data collection activities from Presidential Authorization to FISA authority. Bradbury told the OIG that because it was believed that Judge Howard's Orders, particularly the foreign selectors Order, provided the NSA sufficient flexibility to conduct content collection, it was not necessary to renew the December 8, 2006, Presidential Authorization. ~~(TS//STLW//SI//OC/NF)~~

Therefore, on February 1, 2007, the Presidential Authorization for the Stellar Wind program officially expired.[299] ~~(TS//SI//NF)~~

F. First Domestic and Foreign Selectors FISA Renewal Applications ~~(TS//SI//NF)~~

Judge Howard's January 10, 2007, Orders were set to expire after 90 days. During the week of March 20, 2007, the government filed renewal applications to extend the authorities both as to domestic and foreign selectors. These applications were filed with Judge Roger Vinson, the FISA Court duty judge that week. ~~(TS//SI//NF)~~

The domestic selectors application, filed March 22, 2007, was in all material respects identical to the government's original application. Judge Vinson granted the application on April 5, 2007.[300] ~~(TS//SI//NF)~~

The foreign selectors application was filed on March 20, 2007. The content and construction of the March 20 application was substantially identical to the government's original application, and advanced the same broad construction of the term "facilities" and the use of minimization procedures to authorize NSA officials, instead of judges, to make probable cause determinations (subsequently reviewed by the FISA Court) about particular selectors. ~~(TS//SI//NF)~~

On March 29, 2007, Judge Vinson orally advised the Department that he could not grant the foreign selectors application. His decision validated some concerns within the Justice Department that Judge Howard's original

---

[299] On January 17, 2007, Attorney General Gonzales sent a letter to Senators Leahy and Specter, the Chairman and Ranking Member of the Senate Judiciary Committee, informing them of Judge Howard's Orders. Gonzales's letter stated that as a result of the January 10, 2007, FISA Court Orders, any electronic surveillance that was occurring under the Terrorist Surveillance Program would now be conducted under FISA, and that "the President determined not to reauthorize the Terrorist Surveillance Program when the current authorization expires." ~~(TS//SI//NF)~~

[300] As noted previously, the domestic selectors Order presented special coordination issues between the FBI and the NSA, and [redacted] The Order was renewed for the final time in [redacted] and has since expired. ~~(TS//SI//NF)~~

Order might not be a sustainable long-term strategy for intercepting the communications of foreign selectors. Judge Vinson's decision also accelerated the Department's efforts to obtain legislation amending the FISA statute to authorize the type of surveillance conducted under Stellar Wind and that was approved by Judge Howard. ~~(TS//SI//NF)~~

On April 3, 2007, Judge Vinson issued an Order and Memorandum Opinion explaining the reasoning for his conclusion that he could not grant the foreign selectors application. However, Judge Vinson did not deny the government's application. Instead, he encouraged the Department to file a motion with Judge Howard requesting a 60-day extension of the existing January 10, 2007, foreign selectors Order. In explaining why he was encouraging the Department of file the motion with Judge Howard, Judge Vinson wrote,

> I have concluded that an extension for this purpose is appropriate, in view of the following circumstances: that the government has commendably devoted substantial resources to bring the NSA's surveillance program, which had been conducted under the President's assertion of non-FISA authorities, within the purview of FISA; that a judge of this Court previously authorized this surveillance in [the January 10, 2007, foreign selectors Order], on substantially the same terms as the government now proposes; that it would be no simple matter for the government to terminate surveillance of [redacted] phone numbers and e-mail addresses under FISA authority, and to decide whether and how it should continue some or all of the surveillance under non-FISA authority; and, importantly, that within the allotted time the government may be able to submit an application that would permit me to authorize at least part of the surveillance in a manner consistent with this order and opinion. ~~(TS//SI//NF)~~ b1, b3, b7E

Judge Vinson wrote that the Department's foreign selectors renewal application concerns an "extremely important issue" regarding who may make probable cause findings that determine the individuals and the communications that can be subjected to electronic surveillance under FISA. In Judge Vinson's view, the question was whether probable cause determinations are required to be made by the FISA Court through procedures established by statute, or whether the NSA may make such determinations under an alternative mechanism cast as "minimization procedures." Judge Vinson concluded, based on past practice under FISA and the congressional intent underlying the statute, that probable cause determinations must be made by the FISA Court. ~~(TS//SI//NF)~~

In explaining his reasoning, Judge Vinson first rejected the Department's broad construction of the term "facilities," concluding that the "electronic surveillance" under the government's application – the acquisition of the content of communications – was directed at particular telephone numbers and e-mail addresses, and not at broad swaths of communications [redacted], as the government contended. Judge Vinson distinguished prior cases that the government cited for its broad interpretation of "facilities," observing, "[t]ellingly, none of the cited cases stand for the proposition on which this application rests – that electronic surveillance is not 'directed' at particular phone numbers and e-mail addresses, [redacted]." ~~(TS//SI//NF)~~ b1, b3, b7E

Judge Vinson wrote that his conclusion was also supported by the government's and the Court's past practice, as well as the legislative history of FISA, which, according to Judge Vinson, made clear that "Congress intended the pre-surveillance 'judicial warrant procedure,' and particularly the judge's probable cause findings, to provide an 'external check' on executive branch decisions to conduct surveillance." He wrote that the government's proposal that "the Court assess [redacted] and make a highly abstract and generalized probable cause finding [redacted]" removed from the Court's pre-surveillance purview the question of whether the communications to be acquired will relate to the targeted foreign powers.[301] ~~(TS//SI//NF)~~

Judge Vinson rejected the government's "minimization probable cause standard," stating that "[m]inimization does not provide a substitute for, or a mechanism for overriding, the other requirements of FISA." Judge Vinson concluded that government's proposed minimization procedures, by authorizing the NSA to make probable cause decisions, conflicted with specific provisions of FISA that govern electronic surveillance, such the requirement that only the Attorney General can grant emergency approvals to conduct surveillance (followed within 72 hours by an application to the

---

[301] Stated another way, "[the application] represented that NSA will make the required probable cause finding for each such facility before commencing surveillance." Judge Vision wrote, "[t]he application seeks, in effect, to delegate to the NSA the Court's responsibility to make such findings 'based on the totality of circumstances.' Obviously, this would be inconsistent with the statutory requirement and the congressional intent that the Court make such findings prior to issuing the order (emphasis in original)." ~~(TS//SI//NF)~~

FISA Court), and that renewals for surveillance coverage must be based on "new findings" of probable cause by a judge. Judge Vinson summarized his position:

> The clear purpose of these statutory provisions is to ensure that, as a general rule, surveillances are supported by judicial determinations of probable cause before they commence; that decisions to initiate surveillance prior to judicial review in emergency circumstances are made at politically accountable levels; that judicial review of such emergency authorizations follows swiftly; and that decisions to continue surveillance receive the same degree of scrutiny as decisions to initiate. The law does not permit me, under the rubric of minimization, to approve or authorize alternative procedures to relieve the government of burdensome safeguards expressly imposed by the statute. ~~(TS//SI//NF)~~

Judge Vinson wrote that he was mindful of the government's argument that the proposed minimization procedures were necessary to provide or enhance the "speed and flexibility" with which the NSA responds to threats, and that foreign intelligence information may be lost in the time it takes to obtain Attorney General emergency authorizations. However, in Judge Vinson's view, FISA's requirements reflected a balance struck by Congress between privacy interests and the need to obtain foreign intelligence information, and until Congress took legislative action on FISA to respond to the government's concerns, the Court must apply the statute's procedures.[302] He concluded that the government's application sought to strike a different balance for the surveillance of foreign telephone numbers and e-mail addresses. Vinson rejected this position, stating, "provided that the surveillance is within FISA at all, the statute applies the same requirements to surveillance of facilities used overseas as it does to surveillance of facilities used in the United States."[303] ~~(TS//SI//NF)~~

---

[302] Judge Vinson stated that he recognized that the government maintained the President may have constitutional or statutory authority to conduct the surveillance requested in the renewal application. Judge Vinson stated, "[n]othing in this order and opinion is intended to address the existence or scope of such authority, or this Court's jurisdiction over such matters." ~~(TS//SI//NF)~~

[303] Judge Vinson wrote in a footnote that the status of the proposed surveillance as being within the scope of FISA was "assumed, but not decided, for purposes of this order and opinion." He continued, "I believe that there are jurisdictional issues regarding the application of FISA to communications that are between or among parties who are all located outside the United States." Judge Vinson suggested that "Congress should also consider clarifying or modifying the scope of FISA and of this Court's jurisdiction with regard to such facilities . . . ." Bradbury told the OIG that Judge Vinson's suggestion was an important spur to Congress's willingness to consider FISA modernization legislation in

(Cont'd.)

Attorney General Gonzales told us that his reaction to Judge Vinson's decision was one of "disappointment" and that the decision "confirmed our concern about going to the [FISA Court]." Gonzales also said he believed the decision was "troubling for purposes of the national security of our country." ~~(TS//STLW//SI//OC/NF)~~

Bradbury told us the government considered several options after Judge Vinson's ruling, including appealing the decision to the FISA Court of Review. However, he said the decision was made to attempt to work with Judge Vinson to craft a revised application and also separately to renew the Administration's efforts to obtain legislation to modernize FISA. ~~(TS//SI//NF)~~

G. Revised Renewal Application for Foreign Selectors and Order ~~(TS//SI//NF)~~

As suggested by Judge Vinson, in April 2007 the Justice Department obtained from Judge Howard an extension of the existing foreign selectors Order until May 31, 2007, to prepare a revised foreign selectors application. In the interim, the Department filed two reports with Judge Vinson describing a new approach to foreign selectors that addressed the concerns expressed in his Opinion, and that sought input from the Court about how best to facilitate the submission of an application that would seek authority to direct surveillance at [redacted] selectors. ~~(TS//SI//NF)~~

On May 24, 2007, the Department filed a revised renewal application seeking to renew, with modifications, the authorities granted in Judge Howard's January 10, 2007, Order. However, the application did not include the broad construction of "facilities" and instead sought authority to conduct electronic surveillance of conventional facilities – telephone numbers and "e-mail [redacted]."[304] The application also did not include the "probable cause minimization standard" approved

---

the summer of 2007. In Section IV below, we summarize this legislation, the Protect America Act, and its successor, the FISA Amendments Act of 2008. ~~(TS//SI//NF)~~

[304] According to the May 24, 2007, application, such uses include Internet communications that are sent to and from a targeted e-mail "address," [redacted] The May 24 application was the [redacted] to use the term "e-mail [redacted]" to describe the facility at which e-mail surveillance would be directed; [redacted] However, according to the application, the government "routinely requests, and the Court authorizes, electronic surveillance using [the e-mail [redacted] descriptor to identify this type of facility." ~~(TS//STLW//SI//OC/NF)~~

by Judge Howard that had the effect of shifting from the FISA Court to the NSA the probable cause determinations about particular selectors. ~~(TS//SI//NF)~~

However, the targets of the government's revised application remained selectors (telephone number and e-mail facilities) reasonably believed to be used outside the United States and for which there is probable cause to believe were being used, or are about to be used, by [redacted] b1, b3, b7E [redacted][305] The application also sought [redacted] and in the same manner as was approved in Judge Howard's Order.[306] ~~(TS//SI//NF)~~

Specifically, the application requested authority to direct surveillance at [redacted] categories of foreign selectors:

- Foreign telephone number and e-mail selectors presently known to the government. This category accounted for a portion of the [redacted] foreign selectors already under surveillance pursuant to Judge Howard's Order.[307]

[redacted]

[305] The May 24, 2007, application explicitly stated that the government was not seeking surveillance authority for any new facilities reasonably believed by the NSA to be used by U.S. persons. The application stated that surveillance of those facilities would be initiated only through FISA's emergency authorization provisions and the streamlined FISA applications approved for domestic selectors. ~~(TS//SI//NF)~~

[306] [redacted] b1, b3, b7E

[307] The government submitted an appendix with the revised renewal application that identified [redacted] facilities and contained the factual basis for the NSA's belief that each of the facilities was being used by a person outside the United States and for which there was probable cause to believe were being used or about to be used by a member or agent of one of the targeted foreign powers. The government had provided Judge Vinson these facilities on a rolling basis during May 2007 for his consideration. The NSA discontinued the surveillance of facilities that were targeted under Judge Howard's Order, but that were not included among the facilities submitted to Judge Vinson for approval. The NSA told the OIG that the decision to discontinue surveillance on these [redacted] facilities largely was a resource decision and that [redacted] facilities figure was the amount the NSA could timely process for filing with the Court. ~~(TS//SI//NF)~~ b1, b3, b7E

[redacted]

- Foreign e-mail selectors (not telephone number selectors) presently unknown to the government but that "refer to" or are "about" known foreign e-mail selectors. This category of surveillance, which the NSA had been conducting under Judge Howard's Order, includes situations where an already targeted e-mail facility is mentioned in the body of a message between two third-party, non-targeted facilities.[308] ~~(TS//SI//NF)~~

According to the application, the [redacted] of surveillance would enable the NSA to initiate surveillance of newly discovered facilities "with the speed and agility necessary to obtain vital intelligence and to detect and prevent terrorist attacks." The application stated,

[redacted]

The collection authorities requested in the renewal application that pertained to currently unknown facilities would, according to the application, address this limitation.[309] ~~(TS//SI//NF)~~

Judge Vinson granted the government's revised renewal application on May 31, 2007. His Order authorized, for a period of 90 days, each of the [redacted] categories of electronic surveillance described above, although the

---

[308] The category presented an issue under FISA in that communications are being acquired because they contain the targeted e-mail selector, and not because there was probable cause to believe the e-mail accounts sending or receiving the communications are used or about to be used by an international terrorist group. In such cases, the surveillance is not "directed at" the targeted e-mail selector. The government argued that such acquisition was still consistent with FISA because, "at the time of acquisition, the NSA has probable cause to believe that the facilities at which the NSA is directing surveillance are being used by the foreign power target." ~~(TS//SI//NF)~~

[309] The government argued that the FISA Court's authority to authorize subsequent collection against new selectors unknown to the government at the time an application was approved is rooted in section 1805(c)(3) of FISA. That provision imposes specific reporting requirements on the government where the FISA Court approves an electronic surveillance in circumstances where the nature and location of each of the facilities at which surveillance will be directed is unknown at the time of the application. ~~(TS//SI//NF)~~

Order defined the precise circumstances under which the NSA could acquire communications falling within the [redacted] category of surveillance.[310] The Order also included reporting schedules with respect to the [redacted] categories of surveillance, for which the government was required to submit newly discovered selectors to the Court. ~~(TS//SI//NF)~~

Judge Vinson initially approved [redacted] foreign selectors under the terms of his May 31, 2007, Order (these selectors were submitted with the government's May 24, 2007, application). Shortly after the Order was issued, the FISA Court decided that the weekly reports filed by the government notifying the Court of newly discovered selectors, as well as the government's motions seeking approval to conduct surveillance on additional selectors, could be filed for review with any member of the Court. As the government received feedback from judges on the first reports and motions that were filed, it observed that judges were applying a more rigorous standard of review to the factual basis supporting the surveillance for each selector than Judge Vinson applied to the [redacted] selectors he approved. The government consequently adjusted the amount of factual information it provided the FISA Court in subsequent reports and motions and ultimately added [redacted] foreign selectors to Judge Vinson's Order. ~~(TS//SI//NF)~~ b1, b3, b7E

According to Bradbury, the more rigorous scrutiny applied by FISA Court judges after Judge Vinson's initial approval [redacted] foreign selectors caused the NSA place only a fraction of the foreign selectors under coverage than it wanted to. This concern, combined with the comparatively laborious process for targeting foreign selectors under Judge Vinson's Order, accelerated the government's efforts to obtain legislation that would amend FISA to address the government's surveillance capabilities within the United States directed at persons located outside the United States. The Protect America Act, signed into law on August 5, 2007, accomplished this objective b1, b3, b7E

[310] [redacted] However, his Order authorized the surveillance of any previously non-targeted e-mail facilities that transmitted e-mail messages containing a targeted e-mail account only when the NSA determined, based on the acquired communication and other intelligence or publicly available information, that there was probable cause to believe the e-mail facility was being used, or was about to be used, by one of the targeted foreign powers. Judge Vinson agreed with the government's position that there was probable cause to believe that Internet communications relating to a previously targeted e-mail facility were themselves being sent or received by one of the targeted foreign powers and could be acquired. Judge Vinson called this holding "novel," but concluded that the decision was "consistent with the overall statutory requirements; it requires the government to promptly report and provide appropriate justification to the Court; and it supplies the Government with a necessary degree of agility and flexibility in tracking the targeted foreign powers." ~~(TS//SI//NF)~~ b1, b3, b7E

and effectively superseded Judge Vinson's foreign selectors Order. The government therefore did not seek to renew the Order when it expired on August 24, 2007. ~~(TS//SI//NF)~~

In the next section, we summarize the effect of the Protect America Act and successor legislation, the FISA Amendments Act of 2008. (U)

IV. The Protect America Act and the FISA Amendments Act of 2008 (U)

In August 2007, the Protect America Act was enacted, amending FISA to address the government's ability to conduct electronic surveillance in the United States of persons reasonably believed to be located outside the United States. This legislation expired on February 1, 2008, but was extended by Congress to February 16, 2008. In July 2008, the FISA Amendments Act of 2008 was enacted, which, among other things, created a comprehensive process under FISA for content collection directed at foreign targets. These two laws modernized the FISA statute as it applied to the acquisition in the United States of communications of persons reasonably believed to be outside the United States. (U)

As discussed in Chapter Three, FISA was enacted in 1978 when most international calls were carried by satellite. The interception of such calls constituted "electronic surveillance" for purposes of FISA only if the acquisition intentionally targeted a U.S. person in the United States, or if all participants to the communication were located in the United States. Thus, government surveillance of satellite communications that targeted foreign persons outside the United States generally was not considered electronic surveillance, and the government was not required to obtain a FISA Court order authorizing the surveillance even if one of the parties to the communication was in the United States. However, in the mid-1980s, fiber optic technology began to replace satellites as the primary means for transmitting international (and domestic) telephone communications. This change brought within FISA's definition of "electronic surveillance" the acquisition of telephone calls to or from a person in the United States if the acquisition occurred in the United States, thereby triggering the requirement that the government obtain FISA Court orders to conduct surveillance that it previously conducted outside of FISA. ~~(TS//SI//NF)~~

Under the Stellar Wind program, the NSA collected international communications [redacted] by targeting facilities (telephone numbers and e-mail addresses) located outside the United States (foreign b1, b3, b7E

selectors).[311] As noted in Chapters Three and Four, the Administration contended that FISA, as supplemented by a subsequent legislative enactment (the AUMF), did not preclude the surveillance activities under Stellar Wind, or in the alternative represented an unconstitutional infringement on the President's Article II authority as Commander in Chief to the extent it conflicted with these collection activities. ~~(TS//STLW//SI//OC/NF)~~

The Justice Department's effort to transfer content collection from presidential authority under Stellar Wind to FISA raised the issue of FISA's application to the acquisition in the United States of communications to or from targeted foreign selectors. The Protect America Act and the FISA Amendments Act, in slightly different ways, addressed this issue by treating the communications of persons reasonably believed to be located outside the United States differently from communications of persons located in the United States.[312] ~~(TS//STLW//SI//OC/NF)~~

A. The Protect America Act (U)

The Protect America Act of 2007, Pub. L. No. 110-55, was a temporary measure signed into law on August 5, 2007.[313] The Protect America Act's chief objective was to exclude from the requirements of FISA the interception in the United States of communications of persons located outside the United States, the category of communications referred to above as "foreign selectors." (U)

The Protect America Act amended FISA so that the interception of foreign selector communications fell outside the statute's definition of "electronic surveillance." Under the original definition of "electronic surveillance," FISA generally applied to any communication to or from a known United States person inside the United States if the communication is acquired by targeting the known United States person.[314] FISA also

---

311 The NSA also targeted under Stellar Wind a much smaller number of facilities located inside the United States (domestic selectors). ~~(TS//STLW//SI//OC/NF)~~

312 The two laws did not substantially affect the provisions of FISA relating to pen register and trap and trace surveillance or to the production of "tangible things." The government continues to collect bulk e-mail and telephone meta data under the PR/TT and Section 215 Orders described in Sections I and II of this chapter. ~~(TS//SI//NF)~~

313 The Protect America Act was set to expire 180 days after its enactment, or on February 1, 2008. However, Congress passed and on January 31, 2008, the President signed a bill to extend the Protect America Act for 15 days while further discussions on new legislation occurred. However, no agreement was reached on new legislation and the Act expired on February 16, 2008. (U)

314 The original FISA definition of "electronic surveillance" included:

(Cont'd.)

applied to the acquisition of other communications (such as communications acquired by targeting persons outside the United States) if the communication was a "wire communication" and the acquisition occurred inside the United States. (U)

The Protect America Act amended FISA by stating: "Nothing in the definition of electronic surveillance . . . shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States." The effect of this amendment was to exclude from the requirements of FISA any communication acquired by targeting a foreign selector, regardless of where the communication was intercepted or whether the communication traveled by wire. As a result, the Act eliminated the need for Judge Vinson's May 2007 foreign selectors Order, because the collection of communications targeted under that Order no longer constituted "electronic surveillance" under FISA and therefore no longer required FISA Court orders.[315] ~~(TS//SI//NF)~~

---

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(20(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. § 1801(f). (U)

[315] [redacted] (Cont'd.)

In the place of individualized FISA Court orders, the Protect America Act also inserted several provisions into the FISA statute to govern the acquisition of communications from persons "reasonably believed to be outside the United States." These provisions authorized the Attorney General and the Director of National Intelligence to acquire foreign intelligence information concerning such persons for up to one year, provided these officials certified that there are reasonable procedures in place for the government to determine that a target is reasonably believed to be outside the United States and that the acquisition of the foreign intelligence therefore is not "electronic surveillance" under the amended definition of the term.[316] The targeting procedures accompanying the certification had to be submitted to the FISA Court for approval, based on the clearly erroneous standard, within 120 days of the Protect America Act's enactment. However, the certification was not required to identify specific facilities or places at which the acquisition of foreign intelligence information would be directed.[317] (U)

In addition, the Protect America Act authorized the Attorney General and the Director of National Intelligence to direct a person (telecommunications carriers) to provide the government with "all information, facilities, and assistance necessary to accomplish the acquisition in such a manner as will protect the secrecy of the acquisition. . . ." Protect America Act, Sec. 2(e). The Protect America Act also authorized the Attorney General and the Director of National

---

[redacted] The Protect America Act addressed this issue by excluding all surveillance directed at persons reasonably believed to be outside the United States. ~~(TS//SI//NF)~~

316 The Attorney General and the Director of National Intelligence also had to certify that the acquisition involves the assistance of a communications service provider; that a "significant purpose" of the acquisition to obtain foreign intelligence information is for foreign intelligence purposes; and the minimization procedures to be used with the acquisition activity comport with 50 U.S.C. § 1801(h). Protect America Act, Sec. 2, codified in FISA at 50 U.S.C. § 1805B(a)(1)-(5). (U)

317 The Protect America Act left unchanged the procedures for acquiring foreign intelligence information by targeting foreign powers or agents of foreign power inside the United States, as well as the procedures under Executive Order 12333 Sec. 2.5 to obtain Attorney General approval before acquiring foreign intelligence information against a U.S. person outside the United States. Thus, FISA orders issued prior to the enactment of the Protect America Act, and FISA orders, including applications for renewals, sought after enactment of the Protect America Act but not pursuant to the Act's amendments (acquisition of foreign intelligence information from targets outside the United States) were still subject to FISA as it existed prior to the Protect America Act. The Protect America Act also provided, by means of an "opt-out" clause, that the government did not have to use the new procedures for new applications and could instead file applications under the provisions of FISA as it existed before the Protect America Act. See Protect America Act, Sec. 6(b). (U)

Intelligence to seek the assistance of the FISA Court to compel compliance with such directives, and implemented procedures for the telecommunications carriers to challenge the legality of any such directives.[318] (U)

The Protect America Act authorized the Attorney General and the Director of National Intelligence to issue orders without individualized FISA Court approval for up to one year targeting persons reasonably believed to be outside the United States. These orders remained in effect beyond the expiration of the Protect America Act on February 16, 2008. (U)

On August 10, 2007, the Attorney General and the Director of National Intelligence filed a certification with the FISA Court, as required under the Protect America Act, relating to surveillance of persons reasonably believed to be outside the United States likely to communicate information concerning [redacted] The certification included directives for assistance to specific telecommunications carriers. ~~(TS//SI//NF)~~ b1, b3, b7E

[redacted] foreign selectors under Judge Vinson's Order were "rolled over" to the new Protect America Act authority. A Deputy Assistant Attorney General in the National Security Division familiar with the transition of Stellar Wind to FISA Court authority told us that the government also began to "build new selectors" under the Protect America Act and worked toward restoring the universe of foreign selectors that were first authorized for tasking under Judge Howard's January 2007 Order when content collection under Stellar Wind initially had migrated to FISA Court authority. ~~(TS//SI//NF)~~ b1, b3, b7E

Although the Department viewed the Protect America Act as an adequate temporary fix to those provisions of FISA seen as outdated because of changes in telecommunications technology, Department officials continued to press Congress for more permanent modernization legislation. (U)

---

318 The Protect America Act also stated that any person providing assistance to the government pursuant to a governmental directive would not be subject to any cause of action for providing such assistance. However, the Protect America Act did not grant retroactive legal immunity to any "person," a term defined in FISA to include "any group, entity, association, corporation, or foreign power." 50 U.S.C. § 1801(m). On August 22, 2008, the FISA Court of Review upheld as constitutional the Protect America Act provision authorizing the Director of National Intelligence and the Attorney General to direct a person to assist the government in implementing the Act. See In Re: Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, No. 08-01. (U)

B. The FISA Amendments Act of 2008 (U)

On July 11, 2008, the President signed the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISA Amendments Act). This legislation, composed of four titles, replaced the Protect America Act with similar but more comprehensive surveillance authority. The provisions of the FISA Amendments Act expire, with limited exceptions, on December 31, 2012. (U)

A chief objective of the FISA Amendments Act was to change the rules for intercepting the electronic communications of persons reasonably believed to be outside the United States when the acquisition occurs in the United States. As discussed above, the Protect America Act accomplished this by amending FISA's definition of "electronic surveillance" to exclude this activity from FISA requirements. The FISA Amendments Act took a different approach. Instead of excluding the activity from the statute's definition of "electronic surveillance," the FISA Amendments Act created a new title in FISA to govern how the government may conduct this electronic surveillance. Under this approach, the FISA Amendments Act, unlike the Protect America Act, distinguishes between the targeting of non-U.S. and U.S. persons reasonably believed to be outside the United States.[319] (U)

For non-U.S. persons, the new title created by the FISA Amendments Act provides for surveillance authority similar to the Protect America Act. Instead of requiring the government to obtain individualized orders from the FISA Court to intercept communications of non-U.S. persons reasonably believed to be outside the United States, the FISA Amendments Act authorized the government to conduct any such interceptions for a period of up to one year provided that it adopts, and the FISA Court approves, general targeting procedures designed to ensure that the new authority is not used

---

[319] The Senate Select Committee on Intelligence (SSCI) prepared a section-by-section analysis of the FISA Amendments Act of 2008 explaining the significance of the FISA Amendment Act's approach. According to the SSCI report, the goal of the Protect America Act in redefining the term "electronic surveillance" was to exclude the surveillance of persons outside the United States from the individualized order requirements of FISA. However, a consequence of the term's redefinition was to broadly exempt foreign surveillance activities both of non-U.S. and U.S. persons outside the United States. The FISA Amendments Act of 2008, instead of adopting the Protect America Act's modified definition of "electronic surveillance," explicitly stated that the targeting of non-U.S. persons outside the United States shall be conducted under the new FISA procedures, which does not require an application for a FISA order. In this way, the FISA Amendments Act accomplished the same goal as the Protect America Act without exempting the targeting of U.S. persons outside the United States from FISA's individualized order requirements. (U)

to direct surveillance at persons within the United States or at U.S. persons outside the United States.[320] (U)

In contrast, to conduct U.S.-based surveillance of U.S. persons reasonably believed to be located outside the United States, the FISA Amendments Act requires the government to obtain individualized FISA Court orders for 90-day periods based on a showing of probable cause to believe that the U.S. person is outside the United States and is a foreign power or an agent, officer, or employee of a foreign power. Such surveillance previously was governed by Executive Order 12333, and required only a certification from the Attorney General, not the FISA Court. (U)

Compared to Stellar Wind, the FISA Amendments Act provides the government broader authority to acquire in the United States, with Court supervision, the communications of non-U.S. persons reasonably believed to be located outside the United States. Under Stellar Wind, the NSA was authorized to collect communications where there was probable cause to believe the communications originated or terminated outside the United States and a party to the communications was al Qaeda or a group affiliated with al Qaeda. Under the FISA Amendments Act, the NSA is authorized to collect in the United States any communications of non-U.S. persons reasonably believed to be located outside the United States, provided a significant purpose of the acquisition pertains to foreign intelligence. [redacted]

~~(TS//STLW//SI//OC/NF)~~

---

320 Like the Protect America Act, in addition to these targeting procedures the certification the government is required to file with the FISA Court must also contain minimization procedures and state that a significant purpose of the acquisition that will be conducted is to obtain foreign intelligence information. However, unlike the Protect America Act the FISA Amendments Act does not limit the FISA Court's review of the targeting procedures to a "clearly erroneous" standard. On August 5, 2008, the government submitted to the FISA Court a certification pursuant to the FISA Amendments Act. On September 5, 2008, the Court approved the certification and the use of the targeting and minimization procedures the government submitted. ~~(S//NF)~~

321 On the other hand, the FISA Amendments Act does not similarly broaden the government's authority to conduct surveillance of U.S. persons reasonably believed to be located outside the United States. The Presidential Authorizations did not distinguish between U.S. and non-U.S. persons, and the NSA was authorized under Stellar Wind to intercept the communications of U.S. persons (domestic selectors) provided the communications originated or terminated outside the United States. ~~(TS//STLW//SI//OC/NF)~~

In Chapter Three, we noted that under certain circumstances technological limitations associated with the e-mail content aspect of the Stellar Wind program caused [redacted] (~~TS//SI//NF~~)

The NSA undertook measures to identify and correct incidents [redacted] under Stellar Wind, and the government described the issue to the FISA Court in the December 2006 application that sought to bring Stellar Wind's content collection under FISA authority. [redacted] (~~TS//SI//NF~~)

[redacted]

V. OIG Analysis (U)

As discussed in this chapter, the government's effort to transition Stellar Wind from presidential authority to FISA, which began in March 2004, eventually resulted in all three baskets of collection being authorized by FISA. While the legal theories supporting this transition were aggressive, we believe that the Department could have and should have pursued transition to FISA as a viable legal alternative earlier than it did, rather than operate aspects of the Stellar Wind program solely under presidential authority for several years. ~~(TS//STLW//SI//OC/NF)~~

In Chapters Three and Four we discussed John Yoo's 2001 and 2002 memoranda concerning the legality of Stellar Wind and his contention that FISA represented an unconstitutional infringement on the President's Commander-in-Chief authority under Article II of the Constitution to conduct electronic surveillance during wartime. We recognize that Yoo's analysis was to some extent a response to the extraordinary circumstances that confronted the federal government immediately after the September 11 terrorist attacks and its effort to take emergency steps to thwart what many officials believed was an imminent second wave of attacks. Yet, even if one agrees with Yoo's Article II analysis and supports the decision to enhance outside the judicial or legislative process the NSA's signals intelligence collection capabilities, we believe there are strong countervailing considerations that favored attempting to transition the program to FISA, especially as Stellar Wind became less a temporary response to the September 11 attacks and more a permanent surveillance tool. ~~(TS//STLW//SI//OC/NF)~~

Chief among these considerations was the Stellar Wind program's substantial effect on privacy interests of U.S. persons. Under Stellar Wind, the government engaged in an unprecedented collection of information concerning U.S. persons. The President authorized the NSA to intercept, without judicial approval or oversight, the content of international communications involving many U.S. persons and the NSA collected large amounts of non-content data about U.S. persons' domestic and international telephone calls and to a lesser extent e-mail communications for possible analysis consistent with the extant Presidential Authorization. We believe the FISA Court, as an Article III court and the judicial authority charged by statute to oversee U.S.-based electronic surveillance and other collection activities affecting U.S. persons for foreign intelligence purposes, was the appropriate entity to monitor and approve such broad acquisitions

of U.S.-person information conducted under Stellar Wind.[322] ~~(TS//STLW//SI//OC/NF)~~

Second, as several Justice Department and NSA officials commented, the FISA statute offered a "firmer footing" for the NSA's collection activities under Stellar Wind. As discussed in Chapter Three and Four, the aggressive assertion of Article II authority on which Stellar Wind was based largely reflected the legal reasoning of a single Justice Department attorney working alone, without adequate review or scrutiny of his analysis. As we also concluded, this led to a flawed legal analysis on which the program rested for several years. This approach also led to a contentious dispute between Department and White House officials in 2004 involving renewal of aspects of the program. By contrast, the FISA statute provided an alternative basis for Stellar Wind-like collection activities that we believe should have been considered, and pursued, much earlier by the Administration. ~~(TS//STLW//SI//OC/NF)~~

In this regard, the White House's strict control over the Justice Department's access to the program lessened the opportunity for lawyers with relevant expertise to advise the Administration on the viability of working within the FISA statute to achieve the same operational objectives as the Stellar Wind program. Moreover, as the limited number of Department read-ins persisted, meaningful consideration of FISA as an alternative to presidential authority for the program was limited.[323] ~~(TS//STLW//SI//OC/NF)~~

---

322 For instance, under Stellar Wind the meta data querying standards did not include restrictions on acquiring data that may have been based solely on the exercise of First Amendment rights. When these activities were placed under the FISA Court's supervision, the Court required that this intelligence-gathering activity adhere to the FISA standard that an e-mail address or telephone number cannot be targeted for acquisition based solely on activities protected by the First Amendment. ~~(TS//STLW//SI//OC/NF)~~

323 [redacted]

We also found there were operational benefits to transitioning Stellar Wind to FISA. The PR/TT and Section 215 Orders to collect e-mail and telephone meta data that were eventually obtained from the FISA Court allowed the government to compel [redacted] the [redacted] telecommunications carriers. [redacted] (TS//STLW//SI//OC/NF) b1, b3, b7E

The transition of Stellar Wind to FISA authority, together with the passage of the Protect America Act, allowed the NSA to begin the process to close, or "de-compartment," the Stellar Wind program. This change, which was not completed until mid-2008, has allowed agents in FBI field offices greater access to information about the telephone numbers and e-mail addresses being provided as leads. As described in Chapter Three, the principal complaint of agents who were assigned [redacted] and [redacted] leads was the lack of detail provided about the nature of the international contacts and the foreign entity allegedly involved with terrorism that was one of the communicants. These details often were not provided because of the highly classified and compartmented nature of the Stellar Wind program. Now that such information is gathered under FISA authority and not compartmented as it was under Stellar Wind, it is classified at a level that allows agents in FBI field offices to gain access to additional details upon request.[324] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

We recognize that Stellar Wind's transition to FISA resulted in the imposition of new responsibilities and conditions on the exercise of these unprecedented collection authorities. In the PR/TT and Section 215 Orders, the FISA Court imposed significant oversight measures that were not required under Stellar Wind. To be sure, the government, particularly the NSA, must devote substantial resources to ensure compliance with these oversight measures. Yet, we believe that such requirements are appropriate, given the massive amounts of data collected and the potential impact on the privacy interests of U.S. persons. ~~(TS//STLW//SI//OC/NF)~~

We also recognize that the transition of content collection from presidential authority to statutory authority under FISA resulted in significant diminution in authorized surveillance activity of the content of communications. We described in this chapter how first under Judge Howard's Order, and then more significantly under Judge Vinson's revised

---

[324] Chapter Six of this report discusses FBI agents' improved access to program-derived information under FISA after the Stellar Wind program was closed. ~~(TS//SI//NF)~~

Order, the NSA placed increasingly fewer foreign selectors under FISA coverage as compared to Stellar Wind. The NSA was tasking [redacted] foreign selectors under Stellar Wind at the time of the first content application in December 2006, but placed [redacted] foreign selectors under surveillance coverage under Judge Vinson's May 2007 Order. National Security Division officials told us that they successfully added approximately [redacted] foreign selectors under the terms of the Court's Order. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

However, we believe that such broad surveillance and collection activities conducted in the United States, particularly for a significant period of time, should be conducted pursuant to statute and judicial oversight, even though this resulted in a diminution of foreign selectors due to resource issues. We also believe that placing the activities under Court supervision provides an important measure of accountability for the government's conduct that is less assured when the activities are both authorized and supervised by the Executive Branch alone.[325] ~~(TS//STLW//SI//OC/NF)~~

In sum, we concluded there were compelling reasons to pursue beginning the process of transitioning the collection activities of Stellar Wind to FISA authority earlier than [redacted] 2004. These included the program's large collection of information about U.S. persons, which warranted judicial oversight; the instability of the legal reasoning on which the program rested for several years; and the substantial restrictions placed on FBI agents' access to and use of program-derived information due to Stellar Wind's highly classified status. We acknowledge that transitioning Stellar Wind's collection activities to FISA would have been an enormously complex and time-consuming effort that rested upon novel interpretations and uses of FISA that not all FISA Court judges would authorize. Nevertheless, the events described in this chapter demonstrate that a full transition to FISA authority was achievable and, and in our judgment, should have been pursued earlier. ~~(TS//STLW//SI//OC/NF)~~

[325] Even Judge Vinson's decision regarding the foreign selectors content application, [redacted] was not without benefit. Judge Vinson's decision reflected what some intelligence officials considered limitations in the FISA statute as it applied to the acquisition of communications in the United States of persons located outside the United States, especially non-U.S. persons. In this way, transitioning Stellar Wind's content collection to FISA helped the government make its case to Congress in concrete, non-hypothetical terms for modernization legislation amending the statute. ~~(TS//STLW//SI//OC/NF)~~

CHAPTER SIX [redacted] (~~S//NF~~)

b1, b3, b7E

The preceding chapters examined the evolution of the Stellar Wind program and its transition from Presidential Authorization to FISA authority. In this chapter, we examine more closely the FBI's involvement in Stellar Wind and the impact the program had on FBI counterterrorism efforts. ~~(TS//STLW//SI//OC/NF)~~

[redacted] is the codename for the project, classified at the Secret level, that the FBI initiated in September 2002 to disseminate Stellar Wind information to FBI field offices in a manner that did not disclose the source of the information or the means by which it was acquired. The FBI originally opened [redacted] as an administrative file to serve as the repository for all communications FBI Headquarters disseminated to FBI field offices relating to Stellar Wind information, as well as all communications FBI Headquarters received from field offices reporting the results of any investigation conducted in response to the "tipped" information originating from Stellar Wind. In November 2006, the FBI opened an investigative file under the name [redacted][326] ~~(TS//STLW//SI//OC/NF)~~

b1, b3, b7E

Section I of his chapter summarizes how the FBI used [redacted] to disseminate Stellar Wind information to FBI field offices. Section II describes the FBI's decision in mid-2003 to make its headquarters-based Communications Analysis Unit (CAU), instead of FBI field offices, responsible for issuing National Security Letters (NSL) to obtain subscriber information for telephone numbers (basket 2 of Stellar Wind) disseminated under [redacted][327] Section III discusses the role the FBI played, beginning in approximately March 2004, in the process to "scrub" international terrorism FISA applications for Stellar Wind information. ~~(TS//STLW//SI//OC/NF)~~

b1, b3, b7E

Section IV of this chapter examines the impact of the information obtained from Stellar Wind on FBI counterterrorism efforts. It first provides statistics concerning the number of tippers the NSA derived from Stellar Wind information – telephony, e-mail, and content – disseminated to FBI

---

[326] As discussed in Chapter Three, [redacted] was preceded by the [redacted] which the FBI created in October 2001 to receive and disseminate Stellar Wind-derived information. ~~(TS//STLW//SI//OC/NF)~~

b1, b3, b7E

[327] The CAU is the successor to the Telephone Analysis Unit (TAU), which the FBI created after the September 11 terrorist attacks to analyze telephone communications. The CAU assumed TAU's responsibilities in late 2002. ~~(S//NF)~~

field offices through the [redacted] process. Next, it describes how FBI field offices generally investigated [redacted] tippers and the typical results of the investigations. The section then summarizes two statistical surveys of meta data tippers the FBI conducted in 2006 to assess the value of Stellar Wind to FBI operations, and describes observations about the program's contribution and value provided by FBI officials and employees in OIG interviews and contained in documents the OIG obtained during the course of this review. In addition, the section examines five FBI international terrorism investigations commonly cited as examples of Stellar Wind's contribution to counterterrorism efforts in the United States.[328] b1, b3, b7E ~~(TS//STLW//SI//OC/NF)~~

Lastly, Section V of this chapter contains the OIG's analysis of [redacted] impact on FBI operations. ~~(S//NF)~~ b1, b3, b7E

I. [redacted] Process ~~(S//NF)~~

The [redacted] process was managed by a group of FBI employees from CAU, designated as "Team 10," who in February 2003 were assigned full-time to the NSA to work on the Stellar Wind program.[329] Team 10 was described to us as a "conduit" and a "curtain" between Stellar Wind and the FBI, in that Team 10's chief responsibility was to disseminate Stellar Wind-derived information to FBI field offices for investigation without disclosing that the NSA was the source of the information or how the NSA acquired the information. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

Team 10 initially was staffed with two FBI special agents (one of whom served as supervisor) and two analysts. The CAU subsequently replaced one agent position with a third analyst and later added a fourth analyst. At the NSA, Team 10 was co-located in a large open space with dozens of NSA and other Intelligence Community personnel assigned to the Stellar Wind program. Each team member was provided a computer with direct access to NSA information associated with Stellar Wind. The NSA told the OIG that Team 10 members worked at the NSA under the authority of the NSA Director and as such were required to adhere to NSA minimization rules and attend the same training as NSA employees. Team 10 members also were provided access to Stellar Wind-related systems and

---

[328] As noted above, our report examines the FBI's role in the Stellar Wind program and does not review the use of the program by other agencies, such as the CIA. ~~(S//NF)~~

[329] The CAU is organized into ten teams, nine of which are responsible for providing communications analysis support to specific field offices and FBI Legal Attaches (Legat). According to an FBI organizational chart, Team 10 supports "Off-site Intelligence Community Special Projects." Team 10 was exclusively responsible for managing [redacted] ~~(S//NF)~~ b1, b3, b7E

databases, and had access from their computers to FBI systems such the Automated Case Support (ACS) system and [redacted] b1, b3, b7E
~~(TS//STLW//SI//OC/NF)~~

The process under [redacted] to disseminate Stellar Wind information was similar to the process the FBI established under the [redacted] described in Chapter Three. In short, the NSA provided Top Secret, compartmented Stellar Wind reports to Team 10, which in turn converted the information into Secret, non-compartmented [redacted] b1, b3, b7E electronic communications (EC) and disseminated the communications, referred to as [redacted] "tippers," to FBI field offices for appropriate action.[330] The [redacted] process was applied, with some differences, to each of Stellar Wind's three "baskets" of information. The vast majority of Stellar Wind reports involved the NSA's analysis of telephony meta data – that is, basic information such as date, time, and duration, about contacts between foreign and domestic telephone numbers for which the NSA determined there was a reasonable articulable suspicion to believe were related to al Qaeda or an affiliated group.[331] ~~(TS//STLW//SI//OC/NF)~~

Each [redacted] EC included a paragraph that summarized the [redacted] project and explained that the CAU could not disclose the source of the information contained in the EC, but that the information came from a "sensitive and highly reliable" source. Each EC also included a paragraph advising the field offices that the information provided by the [redacted] source could be used for "lead purposes only" and could not be "incorporated into any affidavit, court proceeding, FISA application or b1, b3, b7E

[redacted]

[redacted]

unclassified investigative file." In addition, each [redacted] EC assigned a "lead" that instructed the field office what investigative action, if any, should be taken regarding the information provided. We further describe [redacted] leads and FBI field offices' handling of them in Section IV of this chapter. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

Before Team 10 disseminated Stellar Wind-derived information to field offices, an analyst queried FBI databases for relevant information about the telephone number, e-mail address, or individual (in the case of a content report) identified in the Stellar Wind report. These queries often identified, for example, subscriber information the FBI previously obtained for Stellar Wind telephone numbers as part of a prior FBI investigation, or active counterterrorism investigations in which the subscriber to a Stellar Wind-targeted number was the subject or in which the number, and sometimes the subscriber, were referenced. Team 10 analysts also checked public and commercial databases, most commonly in connection with e-mail addresses. These checks sometimes identified the specific [redacted] and any domain names the user of an e-mail address had registered. [redacted] Any such information Team 10 located about a Stellar Wind-derived telephone number or e-mail address was included in the [redacted] EC as a "CAU Comment" or an "Analyst Comment" to differentiate the FBI information from the information provided by the Stellar Wind source.[332] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

Over time, Team 10 began to do more than receive and disseminate program-derived information. For example, Team 10 occasionally submitted telephone numbers to the NSA for possible querying against the database containing the bulk telephony meta data collected under Stellar Wind.[333]

---

[332] In this respect, Team 10 handled Stellar Wind content reports differently from meta data reports. Team 10 analysts typically did not perform additional analytical work on the information provided in Stellar Wind content reports other than to identify any FBI cases to which the information was relevant. For example, a content report might summarize intercepted communications indicating that an acquaintance of the subject of an FBI investigation is traveling to or from the United States. The connection between this Stellar Wind information and the relevant FBI investigation would be reported in the [redacted] EC. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

[333] As described in previous chapters, the purpose of the bulk collection of meta data under Stellar Wind was to allow the NSA to use analytical tools such as contact chaining [redacted] to identify known and unknown individuals associated with al Qaeda or an al Qaeda affiliate. The technique involves querying the telephony or e-mail database with a number or address for which an analyst had a "reasonable articulable suspicion" to believe was used by persons involved in al Qaeda or an al Qaeda affiliate, and then examining any contacts with that number or address. ~~(TS//STLW//SI//OC/NF)~~

The telephone numbers Team 10 provided typically were obtained from the FBI's domestic and international counterterrorism operations, such as a number identified during a phone conversation monitored under FISA or a number found in the address book of a subject arrested abroad. The NSA conducted independent analysis to determine whether telephone numbers (or e-mail addresses) provided by Team 10 met the querying standard established by the Presidential Authorizations that governed Stellar Wind (that is, a reasonable articulable suspicion to believe that communications from the telephone number relate to al Qaeda or an affiliated group).[334] ~~(TS//STLW//SI//OC/NF)~~

Team 10 also contributed to the NSA's drafting process for Stellar Wind reports. Telephone numbers and e-mail addresses identified through queries of the databases that contained the bulk telephony and e-mail meta data were reviewed by NSA analysts to determine whether the contacts should be reported to the FBI in a Stellar Wind report. Team 10 participated in this process by reviewing draft reports and providing any information from FBI databases that might be relevant to this determination.[335] ~~(TS//STLW//SI//OC/NF)~~

We were told that one of the benefits of Team 10's presence at the NSA and its involvement in the Stellar Wind report drafting process was an improvement in the quality of the information disseminated to FBI field offices. For example, the FBI Supervisory Special Agent (SSA) who supervised Team 10 from April 2005 to July 2006 told the OIG that he tried to reduce the NSA's reporting of telephone numbers that were several hops removed from the telephone number linked to al Qaeda or an affiliated terrorist group. He said that he wanted Team 10 to disseminate "solid numbers with value," not numbers with questionable value such as "high volume numbers" (public telephones, for example) and [redacted] The FBI SSA said that the NSA expressed the concern b1, b3, b7E

---

334 Team 10 analysts submitted such telephone numbers to the NSA electronically through "Requests for Information," or RFIs, which is the formal process by which the FBI and other agencies provide leads and request information from the Stellar Wind database. FBI records indicate that from April 2002 to January 2006 the FBI directed [redacted] to NSA analysts for possible analysis under Stellar Wind. The records do not indicate the disposition of each RFI. ~~(TS//STLW//SI//OC/NF)~~

335 The NSA developed formal "checklists" to guide the Stellar Wind report drafting process for telephony and e-mail tippers. The checklists include over 30 steps that NSA analysts were required to complete, and a supervisor had to approve, before a report could be distributed to the FBI or any other Stellar Wind customers (the CIA and National Counterterrorism Center). A significant feature of the checklist from the FBI's perspective was the requirement that NSA analysts check any telephone numbers and e-mail addresses in a draft report with the FBI and "make best effort to include FBI . . . data in [the] tipper." ~~(TS//STLW//SI//OC/NF)~~

that it could not foresee whether any particular contact, although remote, might prevent the next terrorist attack, and did not want to find itself in the position of defending its decision not to pass that number to the FBI. However, he said the NSA took several steps to improve the quality of information such as [redacted] for the domestic contacts that were reported and including analytical judgments about the contacts.[336] ~~(TS//STLW//SI//OC/NF)~~

As discussed in Chapter Five, the government transitioned Stellar Wind's bulk e-mail meta data collection (basket 3) to FISA authority in July 2004 with the Pen Register/Trap and Trace Order, bulk telephony meta data collection (basket 2) in May 2006 with the Section 215 Business Records Order, and content collection (basket 1) in January 2007 when the FISA Court granted the government's domestic and foreign selectors applications. ~~(TS//STLW//SI//OC/NF)~~

However, after the transition was completed the NSA continued to produce reports within the Stellar Wind compartment to the FBI and other program customers, even though the information contained in the reports was derived from the FISA-authorized collection activities. Consequently, the FBI continued to disseminate the information under the [redacted] process. The current Team 10 supervisor told us that this decision, reached after consultation with the FBI's Office of the General Counsel (OGC), was made to adhere to the FISA Court's continuing requirement that international terrorism FISA applications be scrubbed for Stellar Wind information (the procedure for which is described in Section III of this chapter). ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

The NSA received permission to begin the process to close, or "de-compartment," the Stellar Wind program after the Protect America Act was passed in August 2007. In mid-2008, the NSA officially closed the program and discontinued issuing "Stellar Wind" reports. In November 2008, the FBI initiated a new investigative file, [redacted] to disseminate the NSA's FISA-derived information.[337] The Team 10 supervisor b1, b3, b7E

---

[336] The NSA told us that one of the difficulties it faced with the Stellar Wind program was that the NSA was serving two customers – the FBI and the CIA – but had just one set of reporting guidelines. This was so because the NSA traditionally does not provide single-agency reporting except in narrowly defined circumstances. [redacted] ~~(S//NF)~~

[337] According to the FBI memorandum explaining the predication for opening the file, the focus of [redacted] investigation is on known and unknown operatives of [redacted] The memorandum stated that as of August 2008 the FBI had [redacted] open national security investigations related to [redacted] of individuals believed to be associated with [redacted] (Cont'd.) b1, b3, b7E

told us that the dissemination process and the FBI's coordination with the NSA under [redacted] is similar to what occurred under [redacted] However, one notable difference is that the NSA's FISA-derived reports, while classified at the Top Secret/Sensitive Compartmented Information (TS/SCI) level, are not subject to the highly restrictive Stellar Wind compartment designation, which is significant from an operational standpoint. [redacted] ECs, like [redacted] ECs, can only include information classified Secret or lower because the FBI's primary computer network for disseminating communications cannot be used for Top Secret information. Unlike under [redacted] agents in field offices can now request access to additional information about [redacted] leads because agents have the appropriate clearances. As discussed in Chapter Three and addressed below, the chief criticism of [redacted] leads was the lack of detailed information that could be provided to field agents about tippers because of the highly compartmented nature of Stellar Wind. b1, b3, b7E

~~(TS//STLW//SI//OC/NF)~~

II. FBI's Decision to Issue National Security Letters under [redacted] to Obtain Telephone Subscriber Information ~~(S//NF)~~ b1, b3, b7E

From August 2003 to November 2006, as part of the [redacted] process the Communications Analysis Unit (CAU) assumed responsibility from the field offices for requesting National Security Letters (NSL) to obtain subscriber information for [redacted] telephone number tippers.[338] The NSLs were authorized by the FBI's OGC and issued pursuant to the [redacted] project. As discussed below, however, this practice was contrary to applicable FBI investigative guidelines because [redacted] was opened as a non-investigative file and therefore under FBI policy should not have been used as the basis for issuing NSLs. ~~(S//NF)~~ b1, b3, b7E

The FBI uses NSLs to obtain information from third parties such as telephone companies, financial institutions, Internet service providers, and consumer credit agencies. NSLs, authorized by five specific provisions contained in four federal statutes, direct third parties to provide customer account information and transactional records such as telephone toll billing

[redacted] of individuals believed to be associated with [redacted] and [redacted] of [redacted] ~~(S//NF)~~ b1, b3, b7E

[338] Field offices remained responsible for issuing NSLs in connection with e-mail address tippers, which was likely attributable to the comparatively low volume of e-mail tippers and the ability of field offices to handle them expeditiously. ~~(S//NF)~~

records.[339] The OIG issued two reviews in 2007 and 2008 examining the FBI's use of NSLs.[340] (U)

Justice Department investigative guidelines issued by the Attorney General govern the circumstances under which the FBI may use NSLs. The Attorney General guidelines in effect during the Stellar Wind program authorized the FBI to issue NSLs relevant to and in the course of an authorized national security investigation.[341] Further, FBI internal policy distinguishes between "investigative files" and non-investigative "administrative files" (commonly referred to as "control files"). This distinction is not a mere technicality. Investigative files, in the national security context, are opened based on evidence that a person, group, or organization is involved in international terrorism. From October 2003 to September 2008, the Attorney General Guidelines required the FBI to provide summary reports to the Justice Department at the end of each year

---

[339] The four federal statutes are the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422; the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709; the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.; and the National Security Act, 50 U.S.C. § 436(a)(1) (2000). NSLs issued under [redacted] relied on the ECPA statute, which provides that the FBI may obtain subscriber information from a communications service provider if the FBI certifies that the information sought is b1, b3, b7E

> relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.

18 U.S.C. § 2709(b)(2) (2000 & Supp. IV 2005). The statute also permits access to "toll billing records" or "electronic communication transactional records," 18 U.S.C. § 2709(a), but requires a warrant for access to the content of telephone communications. See 18 U.S.C. § 2511 (Wiretap Act) and 3121 (Pen Register Act); see also 18 U.S.C. § 2702(b)(8). (U)

[340] The OIG's first report on NSLs, issued in March 2007, was entitled, *A Review of the Federal Bureau of Investigation's Use of National Security Letters*. The OIG's second report, issued in March 2008, was entitled, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*. (U)

[341] From March 8, 1999, through October 31, 2003, national security investigations were governed by the Attorney General's Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCI Guidelines). The FCI Guidelines were replaced, effective October 31, 2003, with the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines). (U)

The evidentiary standard for initiating an investigation is the same under both sets of guidelines. To open a full investigation, the FBI is required to demonstrate [redacted] A preliminary investigation (or "inquiry," under the FCI guidelines) requires only a showing of [redacted] of such involvement. See NSI Guidelines, Section II.C. (October 31, 2003); FCI Guidelines, Section III.B. (March 8, 1999). ~~(S//NF)~~ b1, b3, b7E

a full national security investigation continues. These requirements helped ensure that there was sufficient, documented predication for investigative activities FBI agents sought to conduct, such as requesting NSLs. ~~(S//NF)~~

Control files, in contrast, are "separate files established for the purpose of administering specific phases of an investigative matter or program." The files do not require any predication and remain open indefinitely without any reporting requirements for national security investigations. For example, the September 2002 EC requesting that a control file [redacted] be opened for Stellar Wind information stated that "a dedicated control file for this project will better serve the specific needs of the special project and will add an additional layer of security for the source." The file has remained open since September 2002 without any official documentation of need or justification. (As discussed below, in November 2006 the FBI opened an [redacted] investigative file; however, the [redacted] control file was not closed at that time.) b1, b3, b7E
~~(TS//STLW//SI//OC/NF)~~

The FBI's National Foreign Intelligence Program (NFIP) Manual states that [redacted][342] Thus, in accordance with the NFIP Manual, it was improper for the FBI to issue NSLs from control files during the Stellar Wind program. ~~(S//NF)~~

The OIG's March 2007 NSL report identified the [redacted] project as one of two circumstances where the FBI was using control files rather than investigative files to issue NSLs. The OIG report concluded that this use was contrary to FBI policy. However, our report also found that the CAU officials involved in the decision to issue NSLs from the [redacted] control file concluded in good faith that the FBI had sufficient predication either to connect the [redacted] NSLs with existing preliminary or full investigations of al Qaeda and affiliated groups or to open new preliminary or full investigations in compliance with Justice Department investigative guidelines. ~~(S//NF)~~ b1, b3, b7E

[redacted]

As part of our review of the FBI's participation in Stellar Wind, we sought additional explanation for the use of NSLs under [redacted] We were told the purpose of having the CAU instead of the field offices obtain approval for the issuance of such NSLs was to make the telephony tippers more "actionable" by ensuring that field offices at a minimum knew the subscribers for the numbers. As described in Chapter Three, the members of the [redacted] (the predecessor to [redacted]) had received complaints from agents in FBI field offices that [redacted] leads lacked direction about how to make investigative use of the telephone numbers and did not provide sufficient information to open national security investigations. This was problematic because leads disseminated under the [redacted] and for a time under [redacted] instructed field offices to obtain subscriber information for tipped telephone numbers. Thus, if agents could not locate the information in FBI or commercial databases, they faced a dilemma about how to proceed in the absence of what they viewed as sufficient predication. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

The CAU's first Unit Chief (who served in an Acting capacity) discussed the problem in an EC distributed in January 2003 that addressed the [redacted] project. The EC stated, b1, b3, b7E

> Depending on the nature of the information provided [in an [redacted] lead], field offices may determine this intelligence could be used to predicate either a criminal investigation or an intelligence investigation of someone in their territory. Some of the [redacted] leads may contain a request for a field office to confirm a subscriber in their territory, if possible, in addition to providing intelligence. The identification of some subscribers might actually require a National Security Letter (NSL) or a Grand Jury subpoena; however, the [redacted] control file would not be the appropriate legal authority for these requests. ~~(S//NF)~~ b1, b3, b7E

The Acting Unit Chief's supervision of the CAU ended in February 2003. In March 2003, another FBI Supervisory Special Agent (SSA) was appointed as the CAU's first permanent Unit Chief. He told us that when he joined the CAU he was aware that field offices sometimes did not obtain subscriber information on tippers because some agents did not believe [redacted] ECs provided sufficient information to open a national security investigation. The Unit Chief disagreed, based in part on his insider knowledge about how Stellar Wind operated. He said that he believed the b1, b3, b7E

[redacted] tippers contained sufficient information to open preliminary investigations and issue NSLs.[343] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

The Unit Chief wanted field offices at a minimum to know the identity of subscribers of tipped telephone numbers. He also said it was important to ascertain the correct identities of the subscribers at the time the tipped calls were placed. The Unit Chief stated that if the field office did not issue an NSL for subscriber information promptly, or if the field office relied only on publicly available information, the passage of time could cause the user of the phone to be misidentified. In addition, the Unit Chief said that even if a tipper did not result in any investigative value at the time of the tip, it nevertheless was important to identify the subscriber in the event the tipper became relevant in the future or to another investigation. For all of these reasons, the Unit Chief said he took steps to make the CAU, instead of the FBI field offices, responsible for issuing NSLs for telephone number tippers under the Stellar Wind program.[344] ~~(TS//STLW//SI//OC/NF)~~

In approximately July 2003, a CAU analyst was read into the Stellar Wind program to process [redacted] NSLs. The analyst told us she questioned the Unit Chief and the Team 10 supervisor about whether it was permissible to issue NSLs out of a control file. The Unit Chief told us that he was not aware at this time that a control file such as [redacted] could not be used to issue NSLs. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

The analyst volunteered to approach FBI OGC and met with Marion "Spike" Bowman of the OGC's National Security Law Unit to discuss this concern. She said she told Bowman that the CAU wanted to know if it could issue NSLs under [redacted] in view of its status as a control file. She said she told Bowman that the NSLs would seek subscriber information only and that field offices would be responsible for seeking related toll billing records if warranted by additional investigation. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

According to the analyst, Bowman said that it would be permissible to issue NSLs out of the [redacted] file as long as only subscriber information was sought. The analyst said she could not recall whether Bowman affirmatively stated that issuing NSLs from a control file would be b1, b3, b7E

---

[343] On January 16, 2003, 2 months before the FBI SSA was appointed Unit Chief of the CAU, Attorney General Ashcroft authorized the FBI to issue NSLs during preliminary investigations. Prior to this time, the FCI guidelines authorized the FBI to issue NSLs only as part of a "full investigation." ~~(S//NF)~~

[344] The Unit Chief told us that he did not believe it was critical at the preliminary stage to also obtain telephone subscribers' calling records, or "toll records," identifying all outgoing and incoming calls. ~~(TS//STLW//SI//OC/NF)~~

permissible or whether he merely agreed that it would be permissible under the conditions the analyst presented.[345] ~~(TS//STLW//SI//OC/NF)~~

Shortly after the meeting, the CAU implemented procedures for requesting that OGC issue NSLs to obtain subscriber information for each [redacted] telephone number tipper disseminated to field offices that the FBI was not already aware of or for which it did not have subscriber information. Under these procedures, the CAU analyst received a copy of each [redacted] EC with telephone number tippers as they were issued by Team 10 and drafted a separate approval EC to the NSLB that repeated this information and requested that the NSLB issue NSLs for the numbers listed. NSLB attorneys were responsible for determining whether the NSL requests were "relevant to an authorized investigation," as required by statute. If the attorneys determined that they were, NSLs were drafted and signed by the Deputy General Counsel for NSLB and forwarded to the CAU for service on the appropriate communications service providers. The providers returned the responsive records to the CAU, which in turn disseminated the information to the appropriate FBI field offices. From August 2003 to November 2006, the CAU issued over 500 NSLs under [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

We interviewed FBI Deputy General Counsel Julie Thomas about NSL issuance practices under [redacted] Thomas was read into Stellar Wind shortly after joining the NSLB in October 2004. She was responsible for reviewing and authorizing [redacted] NSLs requested by the CAU. Thomas said she was familiar with the operational reasons the CAU began issuing NSLs under [redacted] but stated that it was not until the OIG was conducting its first review of the FBI's use of NSLs in 2006 that she learned [redacted] was a control file and the significance of this status as it related to issuing NSLs. Thomas said that the CAU's requests to NSLB to authorize NSLs under [redacted] always identified the specific file number associated with the project and indicated that the CAU had initiated a preliminary inquiry in connection with the NSL request. Thus, in Thomas's view, the NSL being requested was "relevant to" an authorized investigation, as b1, b3, b7E

[345] FBI General Counsel Valerie Caproni told the OIG that she believes Bowman based his guidance to the CAU on the understanding that the NSA, by reporting a tipper to the FBI, already had established a reasonable articulable suspicion that the foreign end of the contact was related to al Qaeda or an affiliated group. Caproni said that in view of the hundreds of al Qaeda investigations the FBI was conducting, Bowman likely concluded it was permissible to issue NSLs under [redacted] for the subscriber information of tippers even if at the time there was not a specific investigation to which each NSL could be connected. The Team 10 supervisor at this time told the OIG that he recalled the decision to issue NSLs from [redacted] was based on [redacted] close relationship to the FBI's ongoing investigations of al Qaeda and affiliated groups. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

required by statute and Justice Department investigative guidelines.[346] ~~(TS//STLW//SI//OC/NF)~~

However, Thomas said she did not believe the [redacted] NSLs were improper even though they were issued from a control file. Thomas stated that the NSLs in fact were relevant to authorized international terrorism investigations in that the FBI was conducting hundreds of investigations of al Qaeda and its affiliates at the time the NSLs issued. Thomas told the OIG that, notwithstanding this position, in November 2006 the FBI converted [redacted] to an "umbrella investigative file" to reflect the program's relationship to international terrorism investigations. ~~(TS//SI//NF)~~ b1, b3, b7E

The OIG reviewed the communication from the CAU opening this investigative file. It stated that a member of the U.S. Intelligence Community [the NSA] reported to the FBI that al Qaeda members and associates are using telecommunications systems to facilitate their terrorist activities, that the FBI has independently determined that this is occurring, and that "inasmuch that Al-Qa'ida is a multi-faceted and international terrorism organization, the FBI has determined it is appropriate to open a full field investigative [sic]." The communication stated that the CAU was using information obtained from the member of the U.S. Intelligence Community to issue NSLs and that the results are disseminated to the appropriate FBI field offices. The communication also advised that all investigative leads associated with the investigation would be titled [redacted] to protect the source of the information and the methods used to obtain the information. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

The FBI currently is taking a similar approach to NSLs under the [redacted] A field office (instead of the CAU) is authorized to issue an NSL under the [redacted] investigative file, even if the field office does not open its own investigation and the tipped domestic telephone number or e-mail address is not relevant to another open investigation. However, NSLs issued under [redacted] can request subscriber information only and may not request transactional records, as was done under [redacted] ~~(TS//SI//NF)~~ b1, b3, b7E

The FBI's decision to restrict [redacted] NSLs in this way was not required by law, but was an operational decision. As discussed below, FBI b1, b3, b7E

[346] The [redacted] file number is [redacted] Thomas told us that she did not realize that the "C" designation stood for "Control File." In addition, in the approval ECs reviewed by the OIG that sought the issuance of NSLs, the CAU stated, among other things, that the [redacted] source" reported telephonic contact between possible al Qaeda or other international terrorism entities and numbers in the United States and that "a preliminary CAU inquiry was conducted for the US telephone numbers reported by this source." ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

field offices addressed most [redacted] tippers by conducting "threat assessments" to determine whether the tipper had a nexus to terrorism and warranted the field office initiating a preliminary or full investigation. The subscriber information for a tipper is sufficient for purposes of completing a threat assessment. The same is true for [redacted] tippers, and the current Team 10 supervisor told us that it would not be a "good business" practice to collect transactional records on a U.S. person unless a threat assessment justified the field office initiating its own preliminary or full investigation of the individual. ~~(TS//SI//NF)~~ b1, b3, b7E

We believe the FBI should have opened an [redacted] investigative file in July 2003 and used it to issue NSLs related to Stellar Wind information. The Justice Department investigative guidelines in effect at that time authorized the FBI to open full investigations of groups for which there were specific and articulable facts to believe were involved in international terrorism, such as al Qaeda. However, the FBI decided to issue Stellar Wind NSLs from an existing control file, which was contrary to FBI internal policy. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

We did not find evidence that officials from the CAU and OGC involved in the decision to use an existing control file to issue NSLs related to Stellar Wind information deliberately tried to circumvent FBI guidelines. The July 2003 rationale for issuing the NSLs out of the control file – the close relationship between the Stellar Wind program and the FBI's ongoing investigations of al Qaeda and affiliated groups – essentially was the reasoning used in November 2006 to open the [redacted] investigative file and in November 2008 to open the [redacted] investigative file. As we found in our March 2007 report concerning the FBI's use of NSLs, the CAU and OGC officials involved in the decision to issue NSLs from the [redacted] control file concluded in good faith that the FBI had sufficient predication either to connect the [redacted] NSLs with existing preliminary or full investigations of al Qaeda and affiliated groups or to open new preliminary or full investigations in compliance with Justice Department investigative guidelines. Nevertheless, the decision violated FBI internal policy. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

III. [redacted] and Scrubbing Process ~~(TS//SI//NF)~~ b1, b3, b7E

As discussed in Chapter Three, the Department implemented a process imposed by the FISA Court to "scrub" FISA applications to account for Stellar Wind-derived information. The objectives of the initial scrubbing process were to determine whether any NSA information contained in international terrorism FISA applications was derived from Stellar Wind and whether any of the facilities (telephone numbers or e-mail addresses) targeted by international terrorism FISA applications were also targeted for

Stellar Wind collection (commonly referred to as dual coverage). ~~(TS//STLW//SI//OC/NF)~~

The scrubbing process was coordinated by the Justice Department and NSA, beginning in February 2002 after Judge Lamberth was read into Stellar Wind. In May 2002, Judge Kollar-Kotelly succeeded Judge Lamberth as Presiding Judge of the FISA Court and continued the scrubbing procedures. However, whereas Judge Lamberth required only that he be notified of applications that contained Stellar Wind information, Judge Kollar-Kotelly required that such information be removed. ~~(TS//STLW//SI//OC/NF)~~

As described in Chapter Four, on March 14, 2004, OIPR Counsel Baker briefed Judge Kollar-Kotelly about the President's decision to sign the March 11, 2004, Presidential Authorization without the Justice Department's certification as to the Authorization's form and legality, and about subsequent changes the Authorization made to the Stellar Wind program. ~~(TS//SI//NF)~~

According to a handwritten letter Judge Kollar-Kotelly drafted to Baker following this meeting, Baker had informed her that the Stellar Wind program [redacted] The letter also stated that Baker informed her that with these changes the Deputy Attorney General agreed to certify the program as to form and legality, and that OLC had prepared a new legal memorandum regarding the legality of Stellar Wind to replace the November 2001 memorandum authored by Yoo. ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly's letter marked the first time her expectations concerning the Department's use of Stellar Wind information in FISA applications was communicated in writing to OIPR. Judge Kollar-Kotelly wrote,

> Although the Court has every confidence in the oral representations of Jim Baker [and] does not have any reason to question his honesty or credibility with the FISC or this judge, I am requesting that representations, previously done orally, now be put in writing that relate to [Stellar Wind] and FISA applications so that there are no misunderstandings.
>
> . . . .
>
> I want to emphasize my position which has been consistent since I came on the FISC in May 2002, the [Stellar Wind] program and FISA applications are to be kept separate, and no

> information direct or indirect, derived or obtained from [Stellar Wind] should be included in FISA applications. Only in this way can the integrity of the process and intelligence collected through FISA applications be maintained.
> ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly also wrote that she would not sign any FISA applications that contained substantive information from Stellar Wind-generated tips or any applications where the Stellar Wind tip was the sole or principal factor for an agency initiating the underlying investigation, "even if the investigation was conducted independently of the tip from [Stellar Wind]." ~~(TS//STLW//SI//OC/NF)~~

Baker told us that this letter was Judge Kollar-Kotelly's preliminary response to the changes in the Stellar Wind program. Through subsequent discussions between Judge Kollar-Kotelly and Baker, and between Baker and other Department and FBI officials, a more flexible arrangement was reached on scrubbing that addressed Judge Kollar-Kotelly's concerns without imposing an absolute prohibition on including certain Stellar Wind-derived information in FISA applications.[347]
~~(TS//STLW//SI//OC/NF)~~

In short, the scrubbing procedures implemented in March 2004, and that continue to the present day, substantially expanded the procedures OIPR originally developed in February 2002.[348] In addition to determining whether any NSA information contained in international terrorism FISA applications was derived from Stellar Wind and whether there was any dual coverage, Judge Kollar-Kotelly required the FBI to determine whether any facility (telephone number or e-mail address) that appeared in a FISA application also appeared in a Stellar Wind report and, if so, whether the FBI had developed, independent of Stellar Wind, an investigative interest in the facility before it was the subject of an [redacted] tipper.[349] This third

b1, b3, b7E

[347] FBI OGC said that it was not until these discussions that the FBI was aware of the scrubbing procedures OIPR had implemented in approximately February 2002 after Judge Lamberth was read into the Stellar Wind program. ~~(TS//SI//NF)~~

[348] The scrubbing procedures described here apply both to NSA information derived from the Stellar Wind program and to information derived from the FISA Court's PR/TT and Section 215 bulk meta data orders. Until mid-2008 when the Stellar Wind program officially was closed, leads the NSA developed from the FISA-authorized bulk meta data collections were disseminated under the Stellar Wind compartment.
~~(TS//STLW//SI//OC/NF)~~

[349] As discussed in Chapter Three, Baker did not believe in May 2002, when he first discussed the subject with Judge Kollar-Kotelly, that such a scrub was possible. Baker told us that by March 2004 he better understood the NSA's and FBI's process for disseminating Stellar Wind information and the agencies' ability to track program-derived tips in a timely manner. ~~(TS//STLW//SI//OC/NF)~~

scrub is coordinated among OIPR, the FBI's National Security Law Branch (NSLB), and Team 10. ~~(TS//STLW//SI//OC/NF)~~

The scrub requires NSLB to compile a list of all "facilities" – telephone numbers and e-mail addresses – that appeared in any draft international terrorism FISA applications.[350] This list is compiled as FISA packages become ready for filing with the Court and is provided to an attorney in NSLB read into the Stellar Wind program. The attorney in turn forwards the facilities list to Team 10 at the NSA. Team 10 checks each facility against the NSA's Stellar Wind reports database to determine whether a listed facility is contained in any Stellar Wind reports and, if so, whether the facility appeared in the tearline portion of a report that was further disseminated to FBI field offices. If both inquiries are positive, Team 10 notes the date of the relevant Stellar Wind report and searches the FBI's Automated Case Support System (ACS) to determine whether the facility appears in ACS and, if so, the date the facility came to the FBI's attention. Team 10 reports the results of these checks to the NSLB attorney for review. ~~(TS//STLW//SI//OC/NF)~~

The NSLB attorney takes one of two steps at this stage. If Team 10's checks are negative – meaning none of the facilities are contained in a Stellar Wind report or contained in information below the tearline of a Stellar Wind report – the NSLB scrub attorney notifies the OIPR attorney and FBI case agent that the FISA application can be cleared for presentation to the FISA Court and that the application can proceed to final processing. If both checks on a facility are positive, the NSLB attorney will try to determine if there is a basis for the Court to allow the information in the application based on the theories, discussed in further detail below, that the FBI had an independent investigative interest in or would have inevitably discovered the facility in question. To determine this, the NSLB attorney researches FBI databases, analyzes records, and attempts to craft an argument under one of these theories. The NSLB attorney then provides this information to OIPR for presentation the Court. If the NSLB attorney cannot find a basis for including the information under either of the theories, and the facility is not essential to the showing of probable cause for the requested FISA coverage, the facility is excised from the FISA application, and processing continues. If the information is important to the probable cause showing, the NSLB attorney discusses with OIPR whether to make the argument to the appropriate FISA Court judge (initially

[redacted]

[350]

Judge Kollar-Kotelly and now, the judge assigned to case) that the facility nevertheless can remain in the application. ~~(TS//STLW//SI//OC/NF)~~

According to the Deputy General Counsel for NSLB, the argument to keep such information in an application is based on "standard Fourth Amendment [exclusionary rule] analysis." The "exclusionary rule" generally holds that where the government obtains evidence in violation of the Fourth Amendment, the court will suppress, or exclude, the evidence from the prosecutor's case-in-chief in a criminal trial. Under the "fruit of the poisonous tree" doctrine, a corollary to the exclusionary rule, any evidence obtained directly or derivatively from the government's improper conduct is also excluded. However, there are several exceptions to the exclusionary rule, two of which were relevant to scrubbing: independent source and inevitable discovery. The independent source exception holds that the exclusionary rule does not bar the use of evidence obtained in violation of the Fourth Amendment if there is also an independent, legal source for the evidence.[351] The inevitable discovery exception applies when evidence obtained in violation of the Fourth Amendment would have been obtained independently had the illegal search not occurred, which the government must prove by a preponderance of the evidence.[352] (U)

Thus, in the scrubbing context, the issue is whether the Stellar Wind information contained in a FISA application should not be excluded, either because the FBI had an investigative basis independent of Stellar Wind for including the information in the application or because the FBI inevitably would have discovered the information in the absence of Stellar Wind. More specifically, under the independent investigative basis exception, if Team 10's search of ACS shows that a facility came to the FBI's attention before the facility appeared in a Stellar Wind report, this fact establishes that the FBI has an independent, non-Stellar Wind factual basis to include the facility in the application.[353] NSLB Deputy General Counsel Thomas told us that in her experience the FBI already is aware of the facility – meaning it appears in ACS or other FBI databases – in nearly every instance that a facility contained in a FISA application also appears in a Stellar Wind report. ~~(TS//STLW//SI//OC/NF)~~

---

[351] See *Segura v. United States*, 468 U.S. 796, 805 (1984). (U)

[352] See *Nix v. Williams*, 467 U.S. 431, 443 (1984). (U)

[353] For example, in one case the NSLB attorney's review of the underlying investigative file showed that the FBI had obtained the telephone number at issue in response to an NSL Letter. Because the NSL was dated earlier than the Stellar Wind report that also contained the telephone number, the FBI had an independent investigative basis for including the number in the FISA application. ~~(TS//STLW//SI//OC/NF)~~

The inevitable discovery exception in the scrubbing context applies when Team 10's check of ACS indicates the FBI was not aware of the facility before the date of the Stellar Wind report containing the facility. Under this approach, the NSLB attorney attempts to demonstrate to OIPR that normal investigative steps in the underlying investigation inevitably would have identified the facility in question. The scrubbing attorney analyzes such case evidence as close associates and other relationships of the subjects of the investigation that could logically lead investigators – through NSLs, for example – to the facility contained in the Stellar Wind report.[354] ~~(TS//STLW//SI//OC/NF)~~

Until January 2006, when the full FISA Court was read into Stellar Wind, Judge Kollar-Kotelly required that all applications the FBI determined contained facilities or information that also appeared in Stellar Wind reports be cleared with her before being filed with the FISA Court. As she wrote in a January 12, 2005, letter to OIPR, "I want to ensure, that, to the extent possible, [Stellar Wind] information is excluded from applications submitted to the FISC and that, if it is necessary to include such information, it is specifically identified to the FISC as derived from [Stellar Wind] collection when the application is presented." OIPR Deputy Counsel Skelly-Nolen – who was read into Stellar Wind on March 12, 2004, but who had been involved in the scrubbing process since 2001 – was responsible, along with Baker, for coordinating this aspect of the scrubbing process and, when warranted, for presenting the argument to the judge that an application containing information that was the subject of a Stellar Wind report to the FBI should nevertheless be approved for filing. ~~(TS//STLW//SI//OC/NF)~~

Skelly-Nolen characterized the applications she presented to Judge Kollar-Kotelly as either "vanilla" or "non-vanilla." Vanilla applications were those for which Skelly-Nolen could confidently represent that the FBI had an independent investigative basis for the facility identified in the application that was the subject of a Stellar Wind report (for example, a facility the FBI learned of through FISA coverage that pre-dated the Stellar Wind report). Skelly-Nolen told us that over time Judge Kollar-Kotelly allowed the vanilla applications to be handled telephonically in an unclassified manner, a departure from her general requirement that the discussions be held in judge's chambers. Non-vanilla applications typically involved those cases that required Skelly-Nolan to demonstrate that the FBI

---

354 For example, in one case a telephone number of a particular business did not appear in an FBI database prior to the date it appeared in a Stellar Wind report. However, the subject of the underlying investigation was the target of an FBI national security investigation, and OIPR argued that the telephone number inevitably would have been connected to the subject through the "natural course of the investigation," possibly from toll records associated with other telephone numbers used by the subject, trash covers and open source information, or physical surveillance. ~~(TS//STLW//SI//OC/NF)~~

inevitably would have discovered the facility in question during the normal course of investigation. Skelly-Nolen said these cases were always discussed with Judge Kollar-Kotelly in person. ~~(TS//STLW//SI//OC/NF)~~

Skelly-Nolen told us that there were instances when Judge Kollar-Kotelly requested additional information to support the proffered theory for including Stellar Wind information in the FISA application. In some cases, Judge Kollar-Kotelly simply struck a line through the paragraphs in the filed application that contained the Stellar Wind-derived information and annotated in the margin, "This section (strike) not considered in evaluation of probable cause," followed by her signature and the date. Skelly-Nolen also said that in one or two cases Judge Kollar-Kotelly required that certain Stellar Wind information arguably necessary for establishing probable cause be removed from the applications.[355] However, in general Judge Kollar-Kotelly accepted OIPR's and the FBI's assessment that there was a non-Stellar Wind investigative basis for the information in question, or that the information inevitably would have been discovered even in the absence of Stellar Wind-derived tips to the FBI. ~~(TS//STLW//SI//OC/NF)~~

After operating under the expanded scrubbing procedures for approximately 6 months, Judge Kollar-Kotelly agreed in November 2004 to allow other FISA Court judges who had not yet been read into the Stellar Wind program to handle scrubbed international terrorism applications. However, Judge Kollar-Kotelly still required that Skelly-Nolen bring to her attention all vanilla and non-vanilla applications so they could be "cleared" before being formally filed. As noted above, it was not until January 2006, when the full FISA Court was read into Stellar Wind, that Skelly-Nolen was able to discuss such cases with other judges. ~~(TS//STLW//SI//OC/NF)~~

Since that time, the basic scrubbing procedure described above has continued. The Office of Intelligence attorney primarily responsible for the process told us that each new FISA application that references a facility that was disseminated under Stellar Wind is brought to the attention of the judge assigned to the case.[356] However, with limited exceptions, the FISA Court judges do not require that the government inform them of renewal applications that contain such facilities so long as they were previously brought to the Court's attention in the initiation application or prior renewal applications. The Office of Intelligence attorney told us that the government

---

[355] According to Skelly-Nolen, Judge Kollar-Kotelly nevertheless allowed OIPR to file these applications and approved them. ~~(TS//STLW//SI//OC/NF)~~

[356] The Office of Intelligence Policy and Review (OIPR) became a part of the Department's National Security Division, which was created in September 2006. As of April 2008, OIPR was renamed the Office of Intelligence. (U)

relies on the independent investigative interest theory in the majority of cases in which it seeks to keep a facility in an application. The attorney also said that from the perspective of the Office of Intelligence the scrubbing process is more manageable today than in the past because the process is better organized, additional personnel have been read into the program, and the FISA Amendments Act of 2008 extended the period of time the government must bring emergency applications to the FISA Court from 72 hours to 7 days. However, from the FBI's perspective, the scrubbing process continues to be burdensome and requires a significant expenditure of time and other resources. ~~(TS//STLW//SI//OC/NF)~~

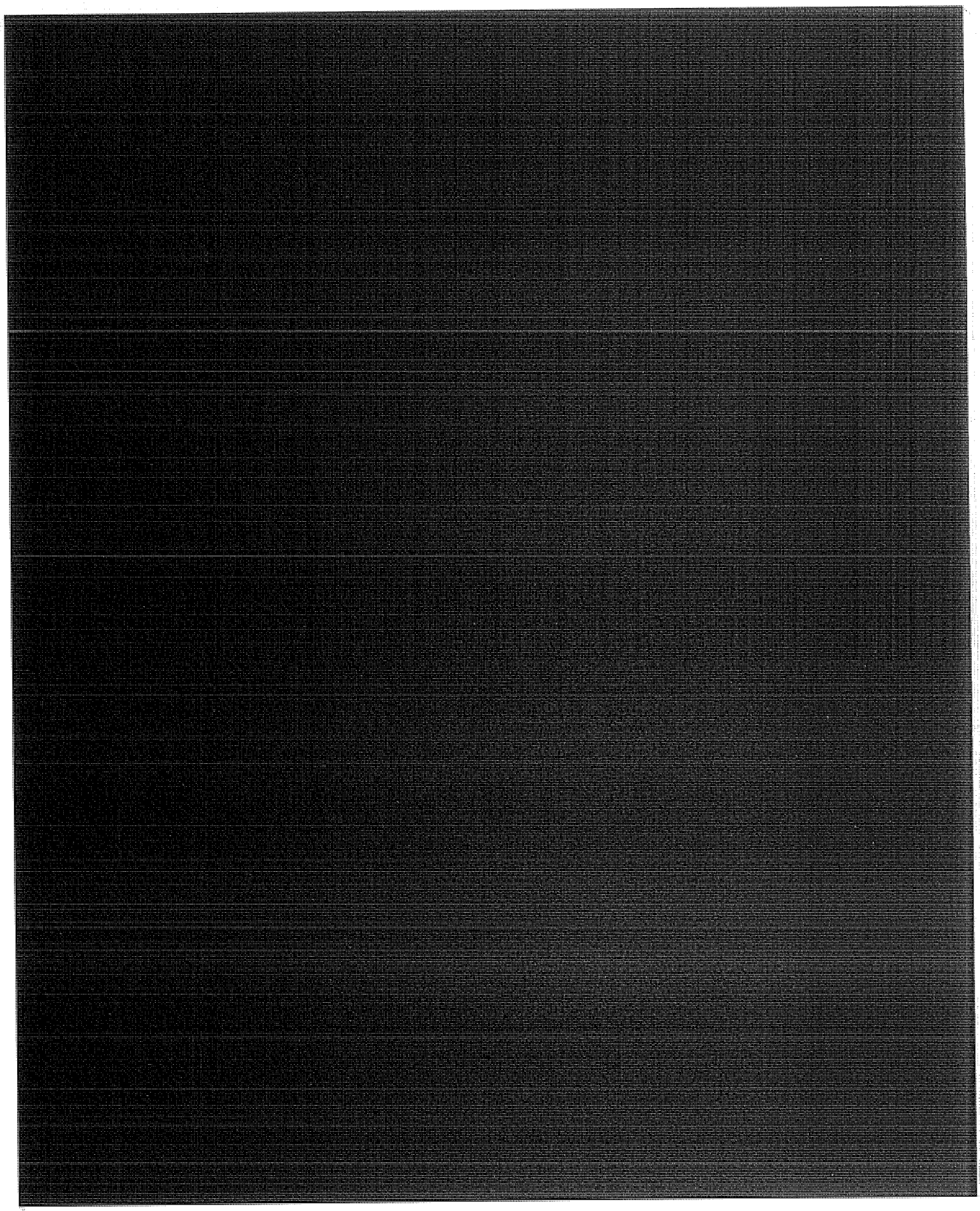
IV. Impact of Stellar Wind Information on FBI Counterterrorism Efforts ~~(S//NF)~~

This section examines the impact of the information obtained from Stellar Wind on FBI counterterrorism efforts. It first provides statistics concerning the number of tippers from Stellar Wind information – telephony, e-mail, and content – disseminated to FBI field offices through the [redacted] process. Next, it describes how FBI field offices generally investigated [redacted] tippers and the typical results of the investigations. This section then summarizes two statistical surveys of meta data tippers the FBI conducted in 2006 to assess the value of Stellar Wind to FBI operations, and describes observations about the program's value provided to us by FBI officials and employees in OIG interviews and contained in documents the OIG obtained during the course of this review. Finally, the section examines [redacted] FBI international terrorism investigations commonly cited as examples of Stellar Wind's contribution to counterterrorism efforts in the United States. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

A. Stellar Wind/[redacted] Statistics ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

We reviewed FBI and NSA statistics relating to the Stellar Wind program. According to an NSA document, from October 1, 2001, to February 28, 2006, the NSA provided [redacted] telephone numbers and e-mail addresses under the Stellar Wind program. The FBI disseminated most of these as tippers to field offices. Chart 6.1 depicts the distribution of the telephone numbers and e-mail addresses the NSA provided the FBI by type. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

b1, b3, b7E



As described in Chapter Three, the NSA provided ratings, or [redacted] for each telephone number and e-mail address to help the FBI prioritize the tippers being disseminated to field offices. The FBI defined the rankings in ECs disseminated to field offices in the following manner:

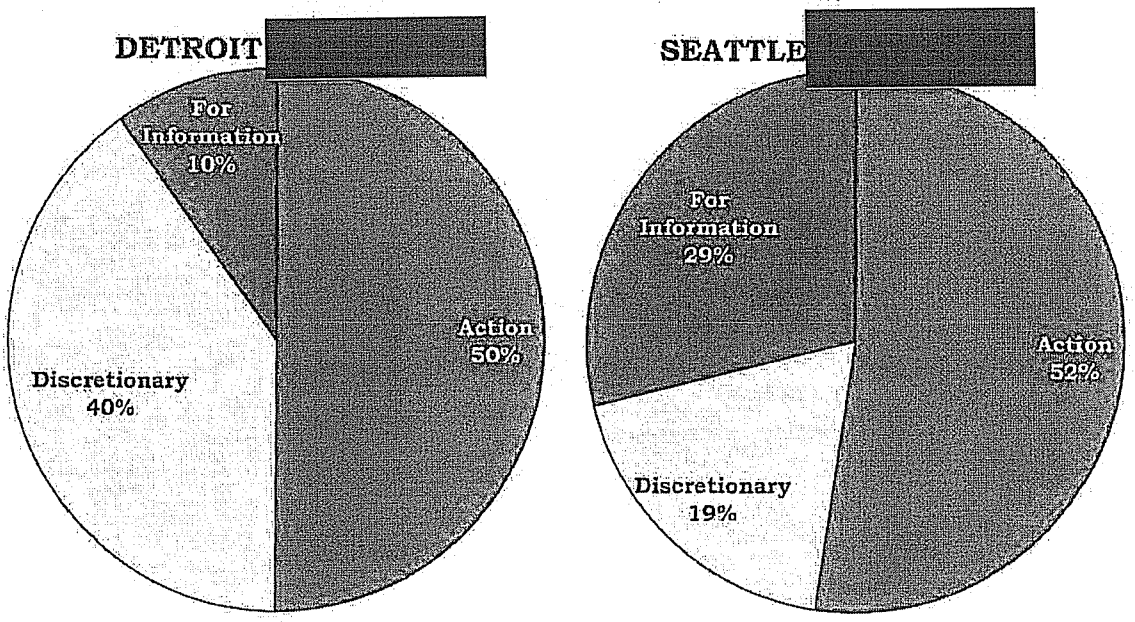
[redacted]

The FBI included these rankings in [redacted] and [redacted] ECs until early 2003. At that time, Team 10 began to make independent assessments about tippers' priority for the FBI, set leads on that basis, and generally discontinued including the ratings in [redacted] ECs. As discussed in this chapter, Team 10 usually set Action leads for telephone numbers and e-mail addresses the FBI did not already know and Discretionary leads for those the FBI was aware of in connection with closed or ongoing cases. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

We could not compare the relationship between the NSA's [redacted] and the FBI's leads because the FBI did not maintain statistics about the lead type for each tipper that Team 10 disseminated. However, in connection with our visits to the FBI's Detroit and Seattle field offices, we examined the number of individual telephone numbers and e-mail addresses provided to those offices and the type of lead assigned for each. We determined that FBI Headquarters assigned Action leads for approximately 50 percent of the total [redacted] leads sent to these offices. As depicted in Chart 6.2, of the [redacted] leads sent to the Detroit field office from December 2001 to December 2006, [redacted] as Action leads. During this same period, of the [redacted] leads sent b1, b3, b7E

to the Seattle field office, [redacted] as Action leads. These figures, taken together with the fact that only 5 percent of the meta data leads the NSA provided the FBI from October 1, 2001, to February 28, 2006, were rated [redacted], indicate that FBI field offices were required to investigate a substantial volume of telephone numbers and e-mail addresses that NSA analysts had rated [redacted] in terms of their connections to terrorism. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

CHART 6.2: Percentage of Lead Types for Detroit and Seattle (January 2001 to May 2007) ~~(S//NF)~~
(Chart below is ~~SECRET//NOFORN~~)



b1, b3, b7E

With respect to leads that provided the content of communications the NSA intercepted under Stellar Wind, the manner in which these leads were disseminated depended on the nature of the communication [redacted]

[redacted].[357] The FBI did not maintain statistics on the number of [redacted] content tippers disseminated to FBI field offices from Stellar Wind content reports. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

We also found that [redacted] leads were distributed unevenly among FBI field offices. The majority of tippers were disseminated to large offices with substantial counterterrorism programs, such as New York, Washington, Chicago, and Los Angeles, and to offices whose territory contained significant Middle Eastern populations, such as Detroit. For example, FBI records indicate that of the [redacted] leads disseminated in 2005, 50 percent were assigned to 10 field offices. Table 6.1 depicts the distribution of [redacted] in 2005 among FBI field offices.[358] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

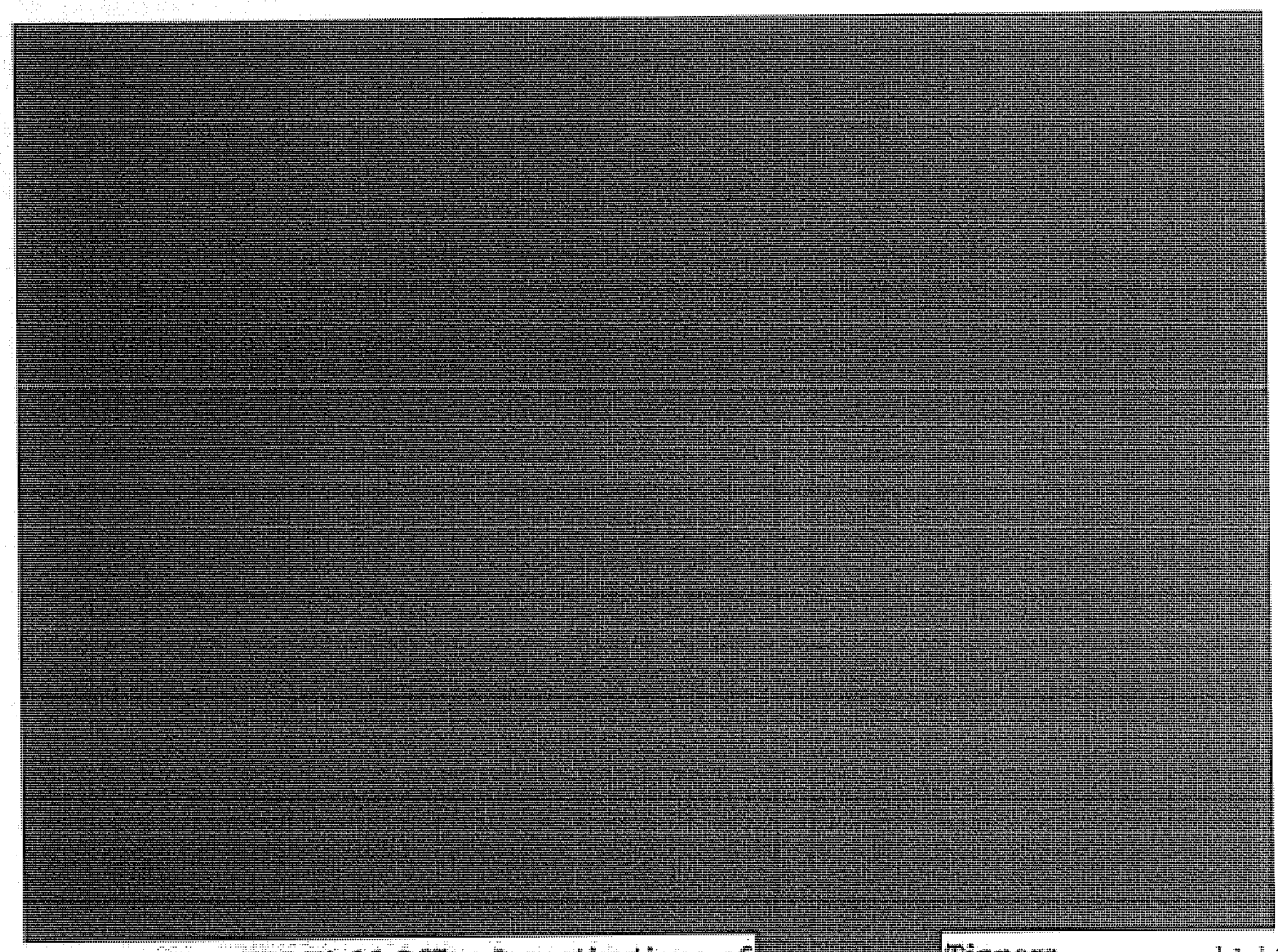
TABLE 6.1: [redacted] Leads by Division (2005) (U//~~FOUO~~) b1, b3, b7E

(Table below is ~~SECRET//NOFORN~~)

[redacted]

[357] [redacted]

[358] A "lead" in these figures does not equate to a single telephone number or e-mail address; each [redacted] lead could contain several telephone numbers or e-mail addresses. For example, the Detroit field office received [redacted] in 2005 containing [redacted] individual tippers. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E



b1, b3, b7E

B. FBI Field Office Investigations of Tippers ~~(S//NF)~~

b1, b3, b7E

FBI field offices were not required to investigate every tipper disseminated under [redacted][359] Rather, the type of lead that the [redacted] EC assigned – Action, Discretionary, or For Information – governed a field office's response to a tipper.[360] [redacted] content tippers, which

b1, b3, b7E

---

[359] As discussed in Chapter Three, the practice under the [redacted] in the first several weeks of the Stellar Wind program was to set Action leads for all telephone number tippers. This practice was modified when the NSA began to designate each tipper in a Stellar Wind report [redacted]

b1, b3, b7E

~~(TS//STLW//SI//OC/NF)~~

[360] An Action lead instructs a field office to take a particular action in response to the EC. An Action lead is "covered" when the field office takes the specified action or conducts appropriate investigation to address the information in the EC. A Discretionary lead allows the field office to make a determination whether the information provided warrants investigative action. A field office that receives a "For Information" lead is not expected to take any specific action in response to the EC, other than possibly route the

(Cont'd.)

provided information derived from communications of telephone numbers and e-mail addresses under surveillance, generally assigned Discretionary or For Information leads. The information in these tippers usually related to individuals already under FBI investigation and was provided to the agents responsible for those cases. [redacted] e-mail address tippers generally assigned Discretionary leads to field offices unless the information was particularly urgent. As noted above, content and e-mail address tippers accounted for a comparatively small portion of the [redacted] tippers disseminated by Team 10. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

The vast majority of FBI investigative activity related to Stellar Wind information involved responding to [redacted] telephone number tippers that assigned Action leads. Team 10 generally assigned Action leads for telephone numbers that the FBI did not previously know or that Team 10 otherwise deemed a high priority, such as a number that had a relationship to a major FBI investigation.[361] From approximately September 2002 (when [redacted] was created) to July 2003, Action leads instructed field offices to obtain subscriber information for the telephone numbers within its jurisdiction and to conduct any "logical investigation to determine terrorist connections." However, some agents complained that these Action leads lacked guidance about how to make use of the tippers, particularly given concerns that the [redacted] communications provided insufficient predication to open national security investigations. b1, b3, b7E
~~(TS//STLW//SI//OC/NF)~~

Two changes in 2003 addressed some of these complaints. First, in July 2003 the CAU assumed responsibility from field offices for issuing NSLs, as we discussed in Section II above. Second, in October 2003 the Attorney General issued new guidelines for FBI national security investigations that created a new category of investigative activity called a "threat assessment."[362] [redacted] b1, b3, b7E

---

communication to the office personnel whose investigations or duties the information concerns. ~~(S//NF)~~

361 Discretionary leads were assigned to telephone numbers that already were known to the FBI, meaning the number or the number's subscriber was referenced in an active FBI investigation. These leads identified the case number of the related investigation and advised receiving field offices to "use the information as deemed appropriate" to bring the information to the attention of the appropriate case agent. ~~(S//NF)~~

362 As noted earlier, the October 2003 guidelines, entitled Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI guidelines), replaced the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations. In September 2008, the Attorney General issued Guidelines for Domestic FBI Operations that replaced the October 2003 NSI guidelines with respect to domestic operations. The September 2008 guidelines use the term "assessment" instead of "threat assessment." (U)

[redacted] b1, b3, b7E

Thus, beginning in October 2003, Action leads assigned by [redacted] telephone number tippers instructed field offices to conduct threat assessments. ~~(TS//STLW//SI//OC/NF)~~

During our review, we visited the Detroit and Seattle field offices to review their handling of [redacted] leads. In addition, we interviewed several supervisory special agents at FBI Headquarters who had experience handling the leads in their respective field offices before being read into the program. In general, these agents' and analysts' experience with [redacted] leads was unremarkable. A threat assessment conducted by these agents and analysts typically involved querying several FBI, public, and commercial databases for any information about the tipped telephone number, and requesting that various state and local government entities conduct similar queries. Sometimes these queries identified the subscriber to the telephone number before the CAU obtained the information with an NSL. In other cases, the threat assessments continued after the field office received the NSL results.[363] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

Examples of the databases utilized in their threat assessments included FBI systems such as the Automated Case Management System and [redacted] other government databases, such as the [redacted] state [redacted] databases, and local police department databases; and commercial databases, such as [redacted] The results of their checks of these databases could sometimes be extensive and include personal information not only about the subscriber to the tipped telephone number, but also about individuals residing in the subscriber's residence or other acquaintances. In other cases, checks were negative or revealed little information about the number or the subscriber. ~~(S//NF)~~ b1, b3, b7E

[363] We were told that it sometimes took [redacted] for field offices to receive subscriber information from the CAU. A Team 10 supervisor said field offices frequently contacted the CAU about the status of outstanding NSLs because the usefulness of threat assessments conducted on a telephone number were limited without the identity of the subscriber. ~~(S//NF)~~ b1, b3, b7E

The agents and analysts said they reviewed the results of these database checks to determine whether additional investigative steps under the threat assessment were warranted or whether there was predication to open a preliminary inquiry. None of the agents we interviewed could recall initiating any investigations based on a threat assessment of an [redacted] tipper.[364] They said they frequently closed [redacted] leads after conducting a threat assessment interview of the subscriber and determining that there was no nexus to terrorism or threat to national security. Alternatively, the leads were closed based solely on the results of database checks. ~~(TS//SI//NF)~~ b1, b3, b7E

Under the Attorney General's October 2003 national security investigations guidelines, [redacted] Under [redacted] agents were not permitted to explain to subscribers how they obtained the information that caused them to seek an interview. Instead, agents simply asked subscribers about their contacts in certain countries and with specific telephone numbers. Agents told us that subscribers generally consented to these interviews and were cooperative and forthcoming. In a few cases, subscribers refused the request or sought the advice of counsel.[366] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

---

[364] Prior to the CAU's July 2003 decision to assume responsibility for issuing NSLs, agents in FBI field offices often opened investigations in order to issue NSLs to obtain subscriber information. These cases usually were closed after the agents conducted investigations and determined the domestic telephone number tipper did not have a nexus to terrorism. ~~(S//NF)~~

[365] On September 29, 2008, the Attorney General issued new guidelines for domestic FBI operations, which includes national security investigations. These guidelines [redacted] *Compare* Attorney General's Guidelines for Domestic FBI Operations, Section II.A.4.f. (September 29, 2008), *with* Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, Section II.A.6. (October 31, 2003). ~~(S//NF)~~ b1, b3, b7E

[366] Several of the threat assessment interviews that agents described to us and that we reviewed in FBI documents provided examples of how some domestic telephone numbers appeared on their face to be in contact with an individual involved in terrorism. In the Seattle field office, several interviews revealed that the foreign telephone calls placed to domestic numbers were made using a pre-paid telephone service from local stores because the callers, often relatives of the domestic contacts, did not have telephone service at their residences. Thus, while the intelligence indicating that an individual involved in terrorism used the foreign telephone number might have been accurate, the number also was used by individuals about whom there was no reason to believe were involved in terrorism. ~~(TS//STLW//SI//OC/NF)~~

FBI field offices were required to report the results of the threat assessments to the CAU. In most of the ECs we reviewed, the field offices reported all of the information that was located about the telephone numbers, including the details of any subscriber interviews, and then stated that the office determined the tipped telephone number did not have a nexus to terrorism and considered the lead closed. Much less frequently, field offices reported that a preliminary investigation was opened to conduct additional investigation.[367] Regardless of whether any links to international terrorism were identified, the results of any threat assessments and the information that was collected about subscribers generally were reported in communications to FBI Headquarters and uploaded into FBI databases. ~~(S//NF)~~

C. FBI Statistical Surveys of [redacted] Meta Data Tippers ~~(TS//STLW//SI//OC/NF)~~

b1, b3, b7E

The FBI made several attempts, both informal and more formal, to assess the value of Stellar Wind to FBI counterterrorism efforts. The first was an informal attempt by the FBI's OGC. FBI General Counsel Valerie Caproni told us that in early 2004 she spoke with the CAU Unit Chief and the Section Chief for the Communications Exploitation Section about trying to assess the value of Stellar Wind information. According to Caproni, the two managers stated that based on anecdotal and informal feedback from FBI field offices, the telephony meta data tippers were the most valuable intelligence from the program for agents working on counterterrorism matters. However, Caproni told us it was difficult to conduct any meaningful assessment of the program's value in early 2004 because FBI field offices at that time were not required to report to FBI Headquarters the investigative results of the Stellar Wind leads disseminated under [redacted] FBI Headquarters did not make such reporting mandatory until October 2004. As a result, Caproni's discussions with the FBI managers did not result in any written assessment of the program. ~~(TS//STLW//SI//OC/NF)~~

b1, b3, b7E

---

[367] The CAU advised field offices that investigative feedback about [redacted] tippers was important because it informed the "reliable source's" (the NSA's) assessment of whether to continue analyzing the "foreign entity" that caused the tippers to be disseminated. An NSA official told us that such information was also important to improving the NSA's analytical process, but he said it was sometimes difficult to obtain such feedback. A CAU Unit Chief told us that the NSA expressed particular concern about insufficient feedback from the FBI regarding investigative results pertaining to the tippers' nexus to terrorism. He said this was a difficult situation in that [redacted] professed to be sending out high value information about known links to terrorism," and it was "uncomfortable" to receive little feedback from field offices other than, "You're sending us garbage." Members of Team 10 told us that efforts to improve field office feedback over time had mixed results. ~~(TS//STLW//SI//OC/NF)~~

b1, b3, b7E

The FBI's second informal assessment of the value of Stellar Wind came after the December 2005 New York Times articles that publicly disclosed the content collection aspect of the Stellar Wind program. Caproni said that in preparation for Director Mueller's testimony at congressional hearings in 2006 on the issue, she attempted to evaluate the Stellar Wind program. Caproni stated that because NSA Director Hayden asserted publicly that the program was valuable, she wanted Mueller's testimony to identify, if possible, any investigations that illustrated Stellar Wind's positive contribution to the FBI's counterterrorism efforts. Caproni stated that this effort was complicated by the fact that Mueller's testimony would be limited only to the aspect of the program disclosed in the New York Times article and subsequently confirmed by the President – the content collection basket. ~~(TS//STLW//SI//OC/NF)~~

As discussed above, Caproni said that FBI field offices did not find this aspect of the program to be as useful as the telephony meta data, primarily because [redacted] was comparatively small and the FBI had FISA coverage on many of these already. Caproni told us that ultimately she was able to identify "a couple" of content tippers that contributed to FBI investigations, but she commented that there were not many. ~~(TS//STLW//SI//OC/NF)~~

The FBI subsequently conducted two more efforts to study the Stellar Wind program's impact on FBI operations, both in early 2006. The first study sampled the [redacted] tippers the FBI had received under Stellar Wind from 2001 through 2005. The second study reviewed [redacted] e-mail tippers the NSA provided the FBI from August 2004 through January 2006. In both of these studies, the FBI sought to determine what percentage of tippers resulted in "significant contribution[s] to the identification of terrorist subjects or activity on U.S. soil." We describe in the next sections the findings of these two studies. b1, b3, b7E
~~(TS//STLW//SI//OC/NF)~~

1. Early 2006 Survey [redacted] Telephony and E-Mail Meta Data Tippers ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

Following the December 2005 New York Times article publicly disclosing the content collection aspect of Stellar Wind, additional members of the Senate and House Intelligence Committees were read into the program. During this time, the NSA provided to cleared members of Congress substantive briefings about Stellar Wind, and the FBI was asked to testify about its participation in the program. In preparation for these briefings and testimony, the FBI sought to quantify the value of Stellar Wind intelligence for FBI counterterrorism operations. The CAU conducted a statistical study for this purpose, and in May 2006 the FBI provided a copy

of the statistical report to the Senate Select Committee on Intelligence. ~~(TS//STLW//SI//OC/NF)~~

The study, conducted during a 1-week period in January 2006, sampled [redacted] unique telephone numbers and e-mail addresses the NSA provided the FBI from the inception of the Stellar Wind program through 2005.[368] The study sought to determine what percentage of the tippers resulted in "significant contribution[s] to the identification of terrorist subjects or activity on U.S. soil." Working with an FBI statistician, the CAU determined that [redacted] randomly selected tippers would be required to obtain statistically significant results. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

Approximately 30 analysts from the FBI's Counterterrorism Division were assigned the task of reviewing [redacted] tippers to determine the disposition of each.[369] The analysts sought to determine whether a particular tipper made a "significant" contribution to FBI counterterrorism efforts. For purposes of the study, a tipper was considered "significant if it led to any of three investigative results: the identification of a terrorist, the deportation from the United States of a suspected terrorist, or the development of an asset that can report about the activities of terrorists." A tipper that led to a field office opening a preliminary or full investigation was not considered "significant" for purposes of the study. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

The analysts researched each tipper's disposition in investigative records contained in FBI electronic databases, beginning with the [redacted] EC that disseminated the tipper to the field. If an analyst concluded based on this research that a tipper was significant, a second analyst who was familiar with the Stellar Wind program further reviewed that determination. If the CAU analyst agreed with the initial finding, the tipper b1, b3, b7E

---

[368] According to the CAU report, the NSA had provided the FBI [redacted] tippers since the inception of Stellar Wind, but [redacted] were duplicates. [redacted] was the total number of unique tippers. The tippers by year were broken down as follows: [redacted] The study also did not include content tippers. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

[369] Most of the analysts were not read into the Stellar Wind program and were told that the study concerned the disposition of [redacted] leads. Of [redacted] tippers reviewed by the analysts, approximately 12 percent were e-mail addresses, a figure consistent with the overall tipper breakdown between e-mail addresses and telephone numbers. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

and supporting information was presented to the CAU Unit Chief for a final review.[370] ~~(TS//STLW//SI//OC/NF)~~

Based on this methodology, the study found that [redacted] 1.2 percent, of [redacted] tippers were "significant." The study extrapolated this figure to the entire population of [redacted] tippers and determined that one could expect to find [redacted] tippers the NSA provided the FBI under Stellar Wind were significant. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

The report documenting the study's findings included brief descriptions of [redacted] "significant" tippers. For example, according to the report, one tipper led to the opening of a full investigation that developed evidence that the user of the tipped e-mail address had "definite ties to terrorism." The user was arrested and pled guilty to charges of [redacted] Another tipper led to the identification of an individual who, [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

Several of the "significant" tippers related to ongoing FBI investigations. For example, information from one tipper designated as significant was already known to the relevant FBI field office, which had an investigation ongoing concerning a subject associated with the tipper prior to receiving the [redacted] EC. According to the study's brief description of the case's significance, the investigative file stated that the tipper was "very beneficial in the on-going investigation" by connecting the subject to terrorism, without describing that connection. Another tipper caused a field office to change a preliminary investigation to a full investigation regarding the possible illegal [redacted] The tipper indicated a connection between one of the subjects of the preliminary investigation and a known terrorist. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

The study also found that 28 percent of [redacted] tippers were never disseminated to FBI field offices for investigation. According to the report, the CAU filtered out these tippers based on "lack of significance" when they were first provided to the FBI by the NSA. These tippers were deemed non-significant for purposes of the study. In addition, the study found that for 22 percent of the sample tippers, FBI field offices did not report any b1, b3, b7E

---

[370] According to a CAU analyst closely involved with the study, establishing a fairly "tight" criteria to identify "significant" tippers was necessary in order to obtain statistically significant results within the one-week time frame the CAU was given to complete the review. The analyst told the OIG that analysts initially applied a broader "significant" standard in their reviews of the tippers, but that it immediately became apparent that a stricter standard was required. The Unit Chief for the CAU told the OIG that the definition of "significant" ultimately used for the study was reached by consensus among Counterterrorism Division operational and analytical personnel. ~~(S//OC/NF)~~

investigative results. The study assumed that the field offices investigated the leads that were set but did not document their work in ACS. These tippers were deemed non-significant for purposes of the study.[371] Thus, combining these two categories, approximately 50 percent of the tippers reviewed as part of the CAU study either were never disseminated to FBI field offices, or were disseminated but with unknown investigative results.[372] ~~(TS//STLW//SI//OC/NF)~~

The FBI's report of the study did not explicitly state any conclusions about whether Stellar Wind was a valuable program. FBI OGC told the OIG that based in part on the results of this study, which found [redacted] of the leads were significant, FBI executive management concluded that the program was "of value." The FBI OGC also said that FBI Director Mueller and Deputy Director Pistole provided congressional testimony in February and May 2006, respectively, about the value of the program, which the FBI OGC stated was based in part on the results of the study. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

2. January 2006 Survey [redacted] E-Mail Meta Data Tippers ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

The CAU conducted a second study of Stellar Wind tippers in January 2006. According to Caproni, this study was in response to a request from the FISA Court about intelligence being obtained pursuant to the July 14, 2004, Pen Register/Trap and Trace Order that authorized the bulk collection of e-mail meta data. As discussed in Chapter Five, e-mail meta data was the first basket of Stellar Wind's signals collection activity that was placed under the FISA Court's authority. However, as noted earlier, the

---

[371] As noted, Caproni cited this lack of reporting from field offices as a reason for not being able to conduct a meaningful assessment of the Stellar Wind program's value in the spring of 2004. FBI Headquarters did not officially require field offices to report investigative results concerning [redacted] tippers until October 2004. According to the CAU analyst with whom the OIG spoke about the study, the idea of contacting field offices to discuss the disposition of tippers and to seek general observations about [redacted] was rejected because of the concern the inquiries might expose the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

[372] By its methodology, the only tippers the study assessed for "significance" were those for which field offices reported investigative results to the CAU and therefore generally did not take into account tippers assigned as Discretionary leads. Discretionary leads, as distinguished from Action leads, did not require field offices to report to the CAU about how the tippers were used. Yet, according to FBI personnel, these leads sometimes were associated with ongoing investigations and sometimes provided new or additional indications of terrorist connections, or reported the content of communications indicating a subject's international movements. The "value" of this category of tippers was not captured in the FBI's study. ~~(TS//STLW//SI//OC/NF)~~

NSA continued to provide e-mail addresses to the FBI in Stellar Wind reports. ~~(TS//STLW//SI//OC/NF)~~

This second study, which reviewed each [redacted] e-mail tippers the NSA provided the FBI from August 2004 through January 2006, applied the same methodology for assessing "significance" that was used in CAU's first study. The second study found that none [redacted] e-mail tippers was "significant" under this standard. The report noted, however, that many of the investigations related to the reviewed e-mail tippers were still ongoing. In addition, the study observed that some of the tippers reviewed had only recently been disseminated to field offices for investigation and that it was possible investigation of these tippers had not been completed. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

D. FBI Judgmental Assessments of Stellar Wind Information ~~(S//NF)~~

To attempt to further assess the value of Stellar Wind information for the FBI, we interviewed FBI Headquarters officials and employees who regularly handled Stellar Wind information. We also interviewed personnel in FBI field offices who were responsible for handling [redacted] tippers. We asked these witnesses for their assessments of the impact of Stellar Wind or [redacted] information on FBI counterterrorism operations. We also recognize that FBI officials and agents other than those we interviewed may have had experiences with [redacted] different than those summarized below. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

The members of Team 10 and its predecessor [redacted] were strong advocates of the program and stated that they believed it contributed significantly to FBI international terrorism investigations. Several claimed that program tippers helped the FBI identify previously unknown subjects, although they were not able to identify for us any specific cases where this occurred. Other witnesses cited the FBI's increased cooperation with the NSA on international terrorism matters as a side benefit of the Stellar Wind program.[373] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

FBI officials and agents from the International Terrorism and Operations Section (ITOS) expressed a more moderate assessment of Stellar Wind. None of the ITOS officials we interviewed could identify significant investigations to which Stellar Wind substantially contributed. However,

---

[373] FBI Deputy General Counsel Julie Thomas also said that Stellar Wind helped improve the relationship between the FBI and CIA. She said the program provided an opportunity to demonstrate the "interoperability of different agencies," and based on her experience dealing with program-related matters the relationship between the FBI and the NSA was "better now than it has ever been." ~~(TS//STLW//SI//OC/NF)~~

they were generally supportive of the program, often stating that it was "one tool of many" in the FBI's fight against international terrorism. ~~(TS//SI//NF)~~

ITOS personnel frequently noted for us the deficiencies in the Stellar Wind information disseminated to field offices, such as the lack of details about the foreign individuals allegedly involved in terrorism with whom domestic telephone numbers and e-mail addresses were in contact. However, these FBI employees believed the possibility that such contacts related to terrorism made investigating the tips worthwhile. Some ITOS witnesses also told us that in their experience the FBI was already aware of many of the [redacted] telephone numbers and e-mail addresses disseminated under [redacted] but that this duplication did not mean the information was without investigative value. For example, one witness said such contacts could "help move cases forward" by confirming a subject's contacts with individuals involved in terrorism or identifying additional terrorist contacts. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

One FBI Headquarters supervisory special agent said that FBI field offices might have been less critical of [redacted] had there been agents in the offices read into Stellar Wind. He said that such agents would have been better positioned than FBI Headquarters' officials to assure others in their respective offices about the reliability of the information being disseminated. A former ITOS section chief told the OIG that he proposed to the NSA that the head of each FBI field office be read into Stellar Wind for this reason and to be able to make fully informed decisions about handling the Stellar Wind tippers. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

The most critical comments we heard about [redacted] impact came primarily from the supervisory special agents we interviewed who managed counterterrorism programs at the two FBI field offices we visited. These agents said the [redacted] tippers and any information developed from the leads might be useful, but that the [redacted] program was not an effective way to identify threats. For example, one supervisor stated that [redacted] represented FBI Headquarters' failure to prioritize threat information. He said that by simply disseminating [redacted] tippers to field offices in ECs that often provided little in the way of details, FBI Headquarters effectively made the field offices "insurance carriers," placing the responsibility solely on them to timely and adequately investigate every lead. The supervisor stated that ordinarily he accepts this responsibility as part of his job, but that the [redacted] tippers were especially frustrating b1, b3, b7E

as compared to other counterterrorism leads the office received because they did not provide sufficient information for him to prioritize the leads.[374]

Another supervisory special agent expressed a similar assessment of [redacted] stating that he felt the project "perverted the logical priority of tasking." He said that absent the leads' special status as part of [redacted] a very low percentage of the tippers would have been considered priority matters. He told us that he did not have the freedom to prioritize the leads in the manner he felt was warranted by the information provided in [redacted] ECs. ~~(TS//SI//NF)~~ b1, b3, b7E

Field office agents who investigated [redacted] leads also were critical of the lack of details contained in [redacted] ECs about the nature of the terrorist connection to the domestic contact, or about the contact itself, such as the duration or frequency of the calling activity. Some agents we interviewed said they also occasionally were frustrated by the prohibition on using [redacted] information in any judicial process, such as in FISA applications, although none could identify an investigation in which the restrictions adversely affected the case. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

Most of the agents we interviewed viewed [redacted] tippers as just another type of lead that required appropriate attention, and the agents generally did not handle the leads with any greater care or sense of urgency than non-[redacted] counterterrorism leads. ~~(TS//SI//NF)~~ b1, b3, b7E

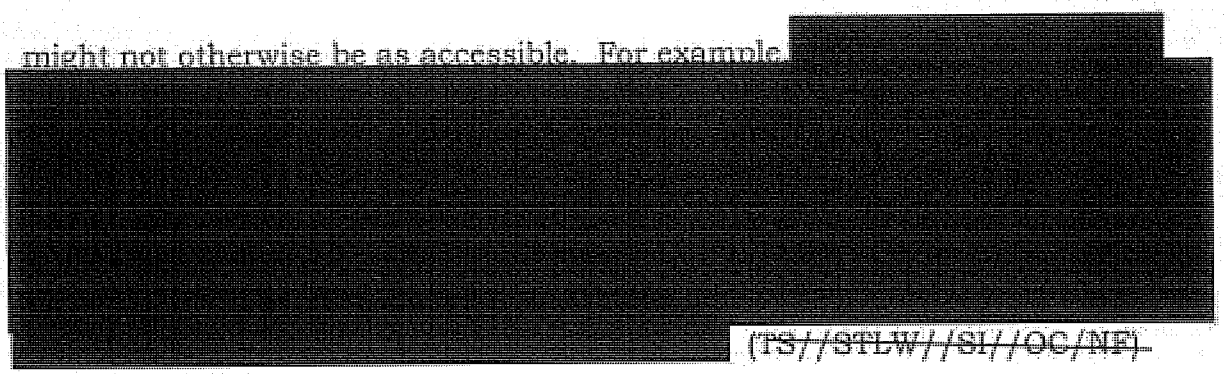
Moreover, none of the agents we interviewed identified an investigation in their office in which [redacted] played a significant role, nor could they recall how such a tipper contributed to any of their international terrorism cases. Nevertheless, the agents generally viewed [redacted] tippers as a potentially valuable source of information, noting that the information developed from the investigations of tippers might prove useful in the future. ~~(TS//SI//NF)~~ b1, b3, b7E

Agents also stated that through the threat assessment interviews they conducted of the subscribers to tipped telephone numbers, [redacted] "opened a window" to populations within the field offices' jurisdiction that b1, b3, b7E

---

[374] The supervisor stated that [redacted] leads had little investigative value to his office. First, he said the leads did not provide enough detail about the reliability of the information being provided. Such details might include, for example, what other individuals had access to the foreign telephone allegedly used by someone involved in international terrorism, and how many calls were made from that number and for what durations. These details would help evaluate the threat represented by the foreign number's contact with the tipped domestic number. Second, the supervisor said the [redacted] tippers lacked direction about what the office should do with a tipped number after a threat assessment has been conducted. ~~(TS//SI//NF)~~ b1, b3, b7E

might not otherwise be as accessible. For example,



~~(TS//STLW//SI//OC/NF)~~

In 2007, FBI Deputy Director John Pistole briefed the Senate Select Committee on Intelligence concerning the FBI's participation in the Stellar Wind program. A document prepared in connection with that briefing addressed, among other subjects, the program's value in FBI national security investigations. The document stated,

> [S]uccessful national security investigations are rarely the result of a single source of information. Rather they occur after exhaustive hours of investigation and the use of legal process in which bits and pieces of intelligence from many sources are gathered and combined into a coherent whole. The *success* or *effectiveness* of any intelligence program – whether Stellar Wind . . . or anything else – is sometimes difficult to assess in the abstract because of that blending of multiple strains of intelligence and because success should never be measured only in terms of terrorist plots that have visibly been disrupted, but also in plots that never formed because our investigative actions themselves had a disruptive effect. (Italics in original.)[375] ~~(TS//STLW//SI//OC/NF)~~

We interviewed FBI Director Mueller in connection with this review and asked him about the value of Stellar Wind to the FBI's counterterrorism program. FBI Director Mueller told us that he believes the Stellar Wind program was useful and that the FBI must follow every lead it receives in order to prevent future terrorist attacks. He said "communications are absolutely essential" to this task and called meta data the "key" to the FBI's

---

[375] A "talking points" document the FBI drafted for Director Mueller also expressed this view. The document stated:

> [The] impact of any single piece of intelligence or program is difficult to quantify. Combination of various information, including humint, sigint, and elsur, is necessary to address the global threat. Accordingly, it is not possible to make an unequivocal "but for" connection between a tip and any particular FBI investigation that has resulted in a seizure or arrest. However, the information has amplified, corroborated and directed FBI investigative resources. ~~(TS//STLW//SI//OC/NF)~~

communications analysis. Mueller also stated that to the extent such information can be gathered and used legally it must be exploited and that he "would not dismiss the potency of a program based on the percentage of hits." Asked if he was familiar with any specific FBI investigations that represent Stellar Wind successes, Mueller said that as a general matter it is very difficult to quantify the effectiveness of an intelligence program without "tagging" the leads that are produced in order to evaluate the role the program information played in any investigation. ~~(TS//STLW//SI//OC/NF)~~

We also asked Mueller about the issue of allocating finite FBI resources to respond to Stellar Wind leads. Mueller said that in the period after the September 11 terrorist attacks, the FBI remained in a state of continuous alert for several years. Mueller stated that he understood the President's desire to take every step to prevent another terrorist attack, and believes that it would be wrong not to utilize all available capabilities to accomplish this, so long as it is done legally. ~~(TS//STLW//SI//OC/NF)~~

Mueller also commented on media reports regarding FBI agents' frustration with the volume of [redacted] leads. For example, articles described complaints of unidentified FBI field agents regarding the lack of information in the tippers they received under [redacted] and how the high volume of tippers necessitated devoting significant resources to what were described as "dry leads."[376] Mueller said that the agents' frustration was similar to that expressed about other sources for the thousands of leads the FBI received after September 11, such as calls from citizens. Mueller stated that he understood the frustration associated with expending finite resources on numerous leads unlikely to have a terrorism nexus, but said that his philosophy after September 11 was that "no lead goes unaddressed." Moreover, he stated that frustrations can result from any counterterrorism program. ~~(S//NF)~~ b1, b3, b7E

We also interviewed Kenneth Wainstein, the first Assistant Attorney General for the Justice Department's National Security Division, which was created in September 2006. Wainstein told us that he was aware of "both sides" on the question of Stellar Wind's value. He also said that he heard the government had not "gotten a heck of a lot out of it," but noted that NSA Director Hayden and FBI Director Mueller have stated that the program was valuable. ~~(S//NF)~~

Hayden told us that he always felt the Stellar Wind program was worthwhile and successful. [redacted]

---

[376] See, e.g., Lowell Bergman, et al., "Domestic Surveillance: The Program; Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," The New York Times, January 17, 2006. (U)

[redacted] Hayden said the FBI believed the leads represented "something certain," when in fact the leads were only "narrow threads" and that the idea was to help build the FBI's intelligence base. Hayden also observed that the enemy may not have been as embedded in the United States as much as feared, but said that he believes Stellar Wind helped determine this. ~~(TS//STLW//SI//OC/NF)~~

E. Examples of FBI Counterterrorism Cases Involving Stellar Wind Information ~~(S//NF)~~

As part of our review, we sought to identify specific FBI international terrorism investigations in which Stellar Wind information was used and to describe the information's specific contributions to the investigations. We agree with FBI officials that this is a difficult task in view of the nature of these investigations, which frequently are predicated on multiple sources of information. To the extent Stellar Wind tips played a role in an investigation, the tips could be one of several sources of information acquired over time and used by the FBI to pursue the investigation. Moreover, the FBI agents and analysts we interviewed during our review could not say that "but for" a Stellar Wind tipper a given investigation would not have been productive, and they were unable to recall specifically how, if at all, Stellar Wind intelligence may have caused their investigations to take a particular direction. ~~(S//NF)~~

Our review did not seek to describe Stellar Wind's impact on each FBI field office, and we recognize that FBI officials and agents other than those we interviewed might have had experiences with [redacted] different than those summarized in this chapter. [redacted] b1, b3, b7E

Because such reporting was not disseminated to FBI field offices under [redacted] any contribution the information might have made to investigations FBI personnel we interviewed were familiar with might not have been accounted for in our questions about Stellar Wind and [redacted] information. ~~(TS//STLW//SI//OC/NF)~~

In view of these difficulties, we examined several investigations frequently cited in NSA and FBI documents the OIG obtained during this

review as examples of Stellar Wind information that contributed to the FBI's counterterrorism efforts.[377] For these investigations, we examined [redacted] ECs, FBI Letterhead Memoranda describing the status of investigative activities in specific cases, Counterterrorism Division responses to OIG questions about the role of [redacted] in specific investigations, government pleadings filed in international terrorism prosecutions, and FBI briefing materials.[378] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

1. [redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted] b1, b3, b6, b7C, b7E

[377] As noted above, the FBI was not the only customer of Stellar Wind information. The CIA and the National Counterterrorism Center also received Stellar Wind reports potentially relevant to their operations. Pursuant to a directive in the FISA Amendments Act of 2008, Intelligence Community OIGs are examining the impact Stellar Wind had on their respective agencies or if Stellar Wind information contributed to their agencies' operations. ~~(TS//STLW//SI//OC/NF)~~

[378] The briefing materials were prepared by the FBI's Communications Exploitation Section (CXS) shortly after aspects of the Stellar Wind program were publicly revealed in a series of New York Times articles in December 2005. The briefing materials were prepared at the direction of FBI General Counsel Valarie Caproni, who anticipated that Director Mueller and Deputy Director Pistole would be called to testify about the program. These briefing materials were intended to help prepare Mueller and Pistole for their testimony. The briefing materials include summaries of specific cases relating to Stellar Wind information that were highlighted by the NSA. ~~(TS//STLW//SI//OC/NF)~~

[redacted] b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

[redacted] This information generated several [redacted] leads for FBI field offices. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

Several of these leads resulted in the FBI initiating investigations of [redacted] to identify any involvement in terrorism. In most cases, the FBI concluded that the individuals' connection [redacted] was not related to any involvement in terrorism. However, in one case FBI investigation determined that the individual was in contact with additional [redacted] engaged in activities indicating possible involvement in terrorist activities.[381] In another case, the FBI b1, b3, b6, b7C, b7E

[379] We described [redacted] in Chapter Three. ~~(S//OC/NF)~~

[380] [redacted] b1, b3, b6, b7C, b7E

[redacted] b1, b3, b7E

[redacted][382] The individual, who had come to the FBI's attention [redacted] but who was not under investigation at the time of the [redacted] tipper, voluntarily departed the country [redacted] (~~TS//STLW//SI//OC/NF~~) b1, b3, b7E

The subject of another of the [redacted] leads generated by [redacted] was already under investigation by an FBI field office. The [redacted] lead caused the FBI office to convert its preliminary investigation into a full investigation and obtain emergency authorization to conduct electronic surveillance under FISA [redacted] used by the individual. The FBI also interviewed the individual several times and issued National Security Letters [redacted] However, the FBI did not develop any information that linked the individual to terrorism or terrorist groups. (~~TS//STLW//SI//OC/NF~~) b1, b3, b7E

2. [redacted] (~~TS//STLW//SI//OC/NF~~)

On [redacted] the FBI's field office [redacted] (~~S//OC/NF~~) b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

[redacted]

b1, b3, b6, b7C, b7E

[redacted]

However, according to documents provided to the OIG, the FBI was [redacted] The FBI therefore was unable to establish that there was a nationwide conspiracy [redacted] to provide material support to terrorism. ~~(S//OC/NF)~~ b1, b3, b7E

Nevertheless, FBI documents state that after [redacted] was closed, field offices with [redacted]-related investigations conducted "successful disruption operations" of criminal activities that were identified during the course of the investigations. ~~(S//OC/NF)~~

3. [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

[redacted]

The FBI's [redacted] opened a full investigation on [redacted] based on his statements [redacted] ~~(S//OC/NF)~~ b1, b3, b6, b7C, b7E

Acting in coordination with [redacted] law enforcement and intelligence agencies, the FBI learned that a group of [redacted] This investigation came to be known by the code name [redacted][384] ~~(TS//SI//OC/NF)~~ b1, b3, b7D b7E

[redacted]

[383] [redacted] b1, b3, b7E

[384] [redacted] b1, b3, b7E

[redacted] b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

[redacted] The EC set a discretionary lead for the FBI [redacted], but encouraged the field office to "provide any pertinent follow-up questions to . . . CAU, for submission to and consideration by the [redacted] source." ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

An FBI response to an OIG request for information about the role of [redacted] in [redacted] case stated that as a result of the [redacted] tipper, the [redacted] located [redacted] after [redacted] return to the United States and established surveillance on [redacted] In an FBI document entitled [redacted] b1, b3, b6, b7C, b7E

---

385 FBI documents we reviewed do not indicate how this information was obtained or whether it was derived from Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

386 The briefing materials state that it could not be verified whether [redacted] ~~(S//OC/NF)~~ b1, b3, b6, b7C, b7E

[redacted]" it is noted that at the time [redacted] returned to the United States the FBI had FISA coverage on [redacted] According to the document, [redacted] [redacted][387] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

FBI briefing materials state that the FBI first began surveillance of an individual later determined to be misidentified [redacted] Through open source investigation, the FBI obtained the telephone number of the misidentified subject and was granted emergency FISA authority on that number. FISA surveillance was initiated on the telephone believed to be used [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

On [redacted] the FBI employees located at the NSA (Team 10) submitted a request to the NSA for call chaining analysis and consideration for Stellar Wind "tasking," or content collection. The NSA initiated content collection on the erroneous telephone number the same day. Contact chaining on the telephone number did not reveal any contacts with any known terrorist-associated numbers. On [redacted] it was determined [redacted] was not using the telephone number tasked and chained under Stellar Wind authority. The FBI also ceased FISA-authorized electronic surveillance of the number [redacted] By [redacted] ongoing physical surveillance confirmed that the telephone number believed to be associated [redacted] had been misidentified. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

On [redacted] the primary suspects in the [redacted] were arrested. [redacted] ~~(S//OC/NF)~~ b1, b3, b6, b7C, b7E

An FBI document stated that since [redacted] arrest [redacted] "has provided a wealth of intelligence to the FBI and the Intelligence Community," and that the intelligence [redacted] provided has been disseminated to intelligence services [redacted] [redacted] ~~(S//OC/NF)~~ b1, b3, b6, b7C, b7D, b7E

[387] A CXS intelligence analyst who drafted the summary of [redacted] for the CXS briefing materials told the OIG that she concluded that the FBI "probably would have figured out eventually" [redacted] was back in the United States based on [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

On [redacted] pled guilty to [redacted] of [redacted] remains incarcerated [redacted]. b1, b3, b6, b7C, b7E

~~(S//NF)~~

[redacted] b1, b3, b6, b7C, b7D, b7E

According to a [redacted] FBI PowerPoint presentation about the FBI's role in Stellar Wind, the [redacted] tipper "facilitated the FBI's ability to locate, initiate physical surveillance, and debrief [redacted] in a timely manner." The facts reviewed by the OIG show that [redacted] failed to result in notification to the FBI of [redacted] return to the United States, but that through Stellar Wind information the FBI was able to locate [redacted] and obtain surveillance of [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

4. [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

According to FBI briefing material, as a result of the [redacted] tipper the [redacted] opened a full international terrorism investigation on [redacted] ~~(S//OC/NF)~~ b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

After receiving the [redacted] tipper in [redacted] the [redacted] requested that FBI Headquarters apply for a FISA order to conduct surveillance of [redacted] The FBI subsequently obtained [redacted] and began FISA electronic surveillance [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

According to an [redacted] Letterhead Memorandum (LHM) drafted by the FBI case agent on [redacted] the FBI determined from [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

---

[389] According to the EC, [redacted] interviewed in connection with the FBI's effort to ascertain [redacted] who the FBI suspected of having ties to [redacted] ~~(S//NF)~~ b1, b3, b6, b7C, b7E

[390] According to the EC, the individual was reported to have told the police [redacted] ~~(S//OC/NF)~~

[redacted] b1, b3, b6, b7C, b7E

The [redacted] LHM described other evidence seized [redacted] In addition, the LHM described additional evidence gathered through several detainee interviews [redacted] ~~(S//OC/NF)~~ b1, b3, b6, b7C, b7E

The FBI arrested [redacted] and an associate [redacted] were indicted on [redacted] indicted on [redacted] ~~(S//NF)~~ b1, b3, b6, b7C, b7E

The arrest and indictment arose out of [redacted] ~~(S//NF)~~ b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

b1, b3, b6, b7C, b7E

[redacted]

b1, b3, b6, b7C, b7E

[redacted]

b1, b3, b6, b7C, b7E

Following [redacted] trial, [redacted] was convicted on [redacted] [redacted] [redacted][393] He was sentenced to [redacted] prison term. ~~(S//NF)~~

In an undated summary of successes under the Stellar Wind program, the NSA characterized [redacted] as

b1, b3, b6, b7C, b7E

[redacted]

b1, b3, b6, b7C, b7E

[redacted]

b1, b3, b6, b7C, b7E

[393] [redacted] was convicted on [redacted] against [redacted]

~~(S//NF)~~

The government's response to the [redacted] stated that the FBI initiated a national security-international terrorism investigation of [redacted] after receiving the [redacted] EC. The government stated that the [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

5. [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

[redacted]

The FBI closed its preliminary investigation of [redacted] after it concluded [redacted] had no nexus to terrorist activities. ~~(S//NF)~~ b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

[redacted] b1, b3, b6, b7C, b7E

According to FBI briefing materials, based on the [redacted] investigation of [redacted] associates [redacted] a FISA order was obtained for [redacted] According to an FBI declaration filed in discovery litigation concerning [redacted] the [redacted] tipper in [redacted] investigation was not used to obtain the FISA order; however, the declaration stated that the tipper [redacted] b1, b3, b6, b7C, b7E

[redacted] (~~TS//STLW//SI//OC/NF~~)

[redacted] was arrested by the FBI later in [redacted] According to the FBI briefing materials, [redacted] b1, b3, b6, b7C, b7E

[redacted] (~~S//OC/NF~~)

On [redacted] the FBI applied for and obtained a FISA order to conduct electronic surveillance and a physical search [redacted] By this time, [redacted] had been in FBI custody for several days.[395] In support of the FISA application, the government reported that [redacted] also in custody at that time, recently had [redacted] b1, b3, b6, b7C b7E

[394] Based on the specific wording of the EC, it is evident that the tipper was derived [redacted] (~~TS//STLW//SI//OC/NF~~) [redacted] b1, b3, b6, b7C, b7E

[redacted] b1, b3, b7E

On [redacted] pleaded guilty to [redacted] b1, b3, b6, b7C, b7E

[redacted][397] ~~(S//NF)~~

The NSA recommended that the FBI cite [redacted] investigation in briefing materials as an example of Stellar Wind's contribution to counterterrorism efforts. The FBI briefing materials also state that the tipper in [redacted] investigation was "instrumental in [redacted] becoming the subject of a Full Investigation on [redacted]" ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

In response to the OIG's request for information about the role [redacted] information played in the investigation [redacted] the FBI's Counterterrorism Division told us [redacted] that, based on its searches of internal FBI databases and discussions with the case agents, "no [redacted] reporting factored into [redacted] investigation." According to a [redacted] declaration the FBI filed in [redacted] prosecution, the [redacted] tipper in [redacted] investigation "did not directly lead to any information or evidence that was used in the prosecution of the case against [redacted] and was not incorporated into any application to a court, including the [FISA Court]."[398] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

[redacted] b6, b7C b7E

[redacted] b1, b3, b6, b7C, b7E

[redacted][399] b1, b3, b6, b7C, b7E

~~(TS//STLW//SI//OC/NF)~~

V. OIG Analysis (U)

The FBI created the [redacted] project to disseminate Stellar Wind information as leads to FBI field offices and assigned the CAU's Team 10 to the NSA to work on Stellar Wind full-time for this purpose. We found that the co-location improved the FBI's knowledge about Stellar Wind operations and gave the NSA better insight about how FBI field offices investigated Stellar Wind information. We were told these benefits translated to improvements in the Stellar Wind report drafting process, and by extension, in [redacted] leads. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

One of the changes the FBI implemented to attempt to improve the investigation of [redacted] leads was to make FBI Headquarters-based CAU, instead of the field offices, responsible for issuing National Security Letters (NSL) to obtain subscriber information on tipped telephone numbers and e-mail addresses. This measure, initiated in July 2003, was intended to address agent concerns that [redacted] leads did not provide sufficient information to initiate national security investigations, a prerequisite under Justice Department investigative guidelines to issuing NSLs. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

However, we found that the CAU issued the NSLs from the [redacted] control file, a non-investigative file created in September 2002 to serve as a repository for [redacted]-related communications between FBI Headquarters and field offices. Issuing the NSLs from a control file instead of an investigative file was contrary to internal FBI policy. The FBI finally opened an investigative file for the [redacted] project in November 2006. We believe the CAU and OGC officials involved in the decision to issue NSLs from the [redacted] control file concluded in good faith that the FBI had sufficient predication either to connect the [redacted] NSLs with existing preliminary or full investigations of al Qaeda and affiliated groups or to open new preliminary or full investigations in compliance with Justice Department investigative guidelines. However, we also concluded that the FBI could have, and should have, opened an investigative file for the [redacted] project when the decision first was made to have FBI Headquarters issue NSLs for [redacted] leads. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

We also described in this chapter a change the FISA Court made in March 2004 to the "scrubbing" process used to account for Stellar Wind information in international terrorism FISA applications. The change requires the FBI's Team 10 and FBI OGC, in coordination with the Department's Office of Intelligence (formerly OIPR), to determine whether any facility (telephone number or e-mail address) that appears in a FISA application also appeared in a Stellar Wind report and, if so, whether the FBI had developed, independent of Stellar Wind, an investigative interest in the facility before it was the subject of an [redacted] tipper, or whether the b1, b3, b7E

facility would have been "inevitably discovered." FISA Court Presiding Judge Kollar-Kotelly imposed this additional scrubbing requirement after being advised of modifications made to Stellar Wind in March 2004 following the Justice Department's revised legal analysis of the program. The FBI and Office of Intelligence continue to expend significant resources to comply with this scrubbing requirement.[399] However, we did not find any instances of the requirement causing the FBI not to be able to obtain FISA surveillance coverage on a target. ~~(TS//STLW//SI//OC/NF)~~

Our primary focus in this chapter was to assess the general role of Stellar Wind information in FBI investigations and its value to the FBI's overall counterterrorism efforts. Similar to the FBI, we had difficulty assessing the specific value of the program to the FBI's counterterrorism activities. However, based on our interviews of FBI managers and agents and our review of documents, and taking into account the substantial volume of leads the program generated for the FBI, we concluded that although the information produced under the Stellar Wind program had value in some counterterrorism investigations, it played a limited role in the FBI's overall counterterrorism efforts. ~~(S//NF)~~

The vast majority of Stellar Wind information the NSA provided the FBI related to telephone numbers and e-mail addresses the NSA identified through meta data analysis as having connections to individuals believed to be involved in international terrorism. The NSA rated a small percentage of these contacts [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

FBI agents and analysts with experience investigating [redacted] leads told us that most leads were determined not to have any connection to b1, b3, b7E

[399] As noted earlier, the scrubbing procedure applies both to NSA information derived from the Stellar Wind program and to information derived from the FISA Court's PR/TT and Section 215 bulk meta data orders. This is so because until mid-2008, when the Stellar Wind program officially was closed, leads the NSA developed from the FISA-authorized bulk meta data collections were disseminated under the Stellar Wind compartment. ~~(TS//STLW//SI//OC/NF)~~

[400] Stated another way, the Stellar Wind program generated [redacted] leads for the FBI each month from October 2001 to February 2006. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

terrorism, and they did not identify for us any specific cases where leads helped the FBI identify previously unknown subjects involved in terrorism (although several stated that this did occur). This is not surprising given that the vast majority of leads sent to FBI field offices for investigation concerned telephone numbers and e-mail addresses that the NSA already had determined were at best one or two steps removed from numbers and addresses suspected of being used by individuals believed to be involved in terrorism. ~~(TS//STLW//SI//OC/NF)~~

The FBI's two statistical studies that attempted to assess the "significance" of Stellar Wind meta data leads to FBI counterterrorism efforts did not include explicit conclusions on the program's usefulness. The first study found [redacted] samples taken from [redacted] meta data leads the NSA provided the FBI from approximately October 2001 to December 2005, [redacted] or 1.2 percent [redacted] made "significant" contributions. The FBI's second statistical study, which reviewed each [redacted] e-mail tippers the NSA provided the FBI from August 2004 through January 2006, identified no examples of "significant" contributions to FBI counterterrorism efforts.[401] The FBI OGC told us that FBI executive management's statements in congressional testimony that the Stellar Wind program had value was based in part on the results of the first study. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

While we believe Stellar Wind's role in FBI cases was limited, assessing the value of the program to the FBI's overall counterterrorism efforts is more complex. Some witnesses commented that an intelligence program's value cannot be assessed by statistical measures alone. Other witnesses, such as General Hayden, said that the value of the program may lie in its ability to help the Intelligence Community determine that the terrorist threat embedded within the country is not as great as once feared. Witnesses also suggested that the value of the program should not depend on documented "success stories," but rather on maintaining an intelligence capability to detect potential terrorist activity in the future. ~~(TS//SI//NF)~~

FBI personnel we interviewed generally were supportive of the Stellar Wind (or [redacted] program, calling the information "one tool of many" in the FBI's anti-terrorism efforts that "could help move cases forward" by, for example, confirming a subject's contacts with individuals involved in terrorism or identifying additional terrorist contacts. However, FBI personnel also frequently noted for us the deficiencies in the Stellar Wind information disseminated to FBI field offices, such as the lack of details b1, b3, b7E

[401] As described earlier in this chapter, the FBI considered a tipper "significant" if it led to any of three investigative results: the identification of a terrorist, the deportation from the United States of a suspected terrorist, or the development of an asset that can report about the activities of terrorists. ~~(TS//STLW//SI//OC/NF)~~

about the foreign individuals allegedly involved in terrorism with whom domestic telephone numbers and e-mail addresses were in contact. Yet, these FBI employees also believed the possibility that such contacts related to terrorism made investigating the tips worthwhile. Some FBI employees also cited the FBI's increased cooperation with the NSA on international terrorism matters as a side benefit of the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

FBI Director Mueller told us that he believes the Stellar Wind program was useful and that the FBI must follow every lead it receives in order to prevent future terrorist attacks. He said "communications are absolutely essential" to this task and called meta data the "key" to the FBI's communications analysis. Mueller also stated that to the extent such information can be gathered and used legally it must be exploited and that he "would not dismiss the potency of a program based on the percentage of hits." ~~(TS//STLW//SI//OC/NF)~~

We sought to look beyond these comments of general support for Stellar Wind to specific, concrete examples of the program's contributions that also illustrated the role Stellar Wind information could play. We therefore examined five cases frequently cited in documents we reviewed and during our interviews as examples of Stellar Wind's contribution to the FBI's counterterrorism efforts. The cases include [redacted] b1, b3, b6, b7C, b7E

[redacted] In another case, Stellar Wind information revealed to the FBI that [redacted] ~~(TS//STLW//SI//OC/NF)~~

In another case [redacted] b1, b3, b6, b7C, b7E

[redacted] According to the FBI, while the Stellar Wind information was either never used or "was of no value" in the criminal investigation that led to [redacted] arrest and conviction, it was an [redacted] tipper that led to the national security investigation that preceded the criminal prosecution. ~~(TS//STLW//SI//OC/NF)~~

The final investigation we examined [redacted] did not appear to result directly from Stellar Wind information. The NSA and the FBI at times have cited [redacted] case as an example of the contributions of Stellar Wind to b1, b3, b6,b7C, b7E

counterterrorism investigations. An FBI declaration filed in [redacted] prosecution indicated that [redacted] Moreover, the FBI told us in response to our inquiry that Stellar Wind information did not "factor into [redacted] investigation." However, we concluded that Stellar Wind may have played some indirect role [redacted] becoming the subject of a Full Investigation by the FBI. Our review of documents indicated that [redacted] investigation, which appears to have been advanced by Stellar Wind reporting, might have caused the FBI to reopen its investigation [redacted] We were unable to describe with the same certainty as in [redacted] investigation the extent of Stellar Wind's contribution to [redacted] investigation, in part because of differing assessments in the FBI's own documents regarding the role of Stellar Wind this matter. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

In short, we found that Stellar Wind generally has played a limited role in FBI counterterrorism investigations, but that the evidence shows there are cases where Stellar Wind information had value. For example, in some of the cases we examined Stellar Wind information caused the FBI to take action that led to useful investigative results. However, in others the connection between the Stellar Wind information and the FBI's investigative actions was more difficult to discern. ~~(S//NF)~~

As discussed in Chapter Five and in this chapter, Stellar Wind's bulk meta data collection activities were transitioned to FISA authority and are ongoing. The FBI, under the [redacted] project (the successor to [redacted]), requires field offices to conduct, at a minimum, threat assessments on telephone numbers and e-mail addresses the NSA derives from this FISA-authorized collection that the FBI is not already aware of, including numbers and addresses one or two steps removed from direct contacts with individuals involved in terrorism. In view of our findings about the Stellar Wind program's contribution to the FBI's counterterrorism efforts, we believe that the FBI should regularly assess the impact [redacted] leads have on FBI field offices and whether limited FBI resources should be used to investigate all of them. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

Another consequence of the Stellar Wind program and the FBI's approach to assigning leads was that many threat assessments were conducted on individuals located in the United States, including U.S. persons, who were determined not to have any nexus to terrorism or

represent a threat to national security.[402] These assessments also caused the FBI to collect and retain a significant amount of personal information about the users of tipped telephone numbers and e-mail addresses. In addition to an individual's name and home address, such information could include where the person worked, records of foreign travel, and the identity of family members. The results of these threat assessments and the information that was collected generally were reported in communications to FBI Headquarters and uploaded into FBI databases. ~~(TS//STLW//SI//OC/NF)~~

The FBI's collection of U.S. person information in this manner is ongoing under the NSA's FISA-authorized bulk meta data collection. To the extent leads derived from this program generate results similar to those under Stellar Wind, the FBI will continue to collect and retain a significant amount of information about individuals in the United States, including U.S. persons, that do not have a nexus to terrorism or represent a threat to national security. ~~(TS//STLW//SI//OC/NF)~~

We recommend that as part of the [redacted] project, the Justice Department's National Security Division (NSD), working with the FBI, should collect information about the quantity of telephone numbers and e-mail addresses disseminated to FBI field offices that are assigned as Action leads and that require offices to conduct threat assessments. The information compiled should include whether individuals identified in threat assessments are U.S. or non-U.S. persons and whether the threat assessments led to the opening of preliminary or full national security investigations. With respect to threat assessments that conclude that users of tipped telephone numbers or e-mail addresses are not involved in terrorism and are not threats to national security, the Justice Department should take steps to track the quantity and nature of the U.S. person information collected and how the FBI retains and utilizes this information. This will enable the Justice Department and entities with oversight responsibilities, including the OIG and congressional committees, to assess the impact this intelligence program has on the privacy interests of U.S. persons and to consider whether, and for how long, such information should be retained. ~~(TS//SI//OC/NF)~~ b1, b3, b7E

[redacted] b1, b3, b7E

We also recommend that, consistent with NSD's current oversight activities and as part of its periodic reviews of national security investigations at FBI Headquarters and field offices, NSD should review a representative sampling [redacted] leads to those offices. For each lead examined, NSD should assess FBI compliance with applicable legal requirements in the use of the lead and in any ensuing investigations, particularly with the requirements governing the collection and use of U.S. person information. ~~(TS//SI//OC/NF)~~ b1, b3, b7E

In sum, we agree that it is difficult to assess or quantify the effectiveness of a particular intelligence program. However, based on the interviews we conducted and documents we reviewed, we found that Stellar Wind information generally played a limited role in the FBI's counterterrorism efforts, but that the information had value in some cases. In addition, some witnesses said the program provides an "early warning system" to allow the Intelligence Community to detect potential terrorist attacks, even if the system has not specifically uncovered evidence of preparations for such an attack. Moreover, other OIGs in the Intelligence Community are reviewing their agency's involvement with the program and the results of those reviews, analyzed together, will provide a more comprehensive picture of the program's overall usefulness. ~~(TS//STLW//SI//OC/NF)~~

Finally, because the bulk meta data aspect of the Stellar Wind program continues under FISA authority, we recommend that the NSD take steps to gather information on the continuing operations of the program, including the use and handling of vast amounts of information on U.S. persons and the effectiveness of the program in FBI counterterrorism investigations. ~~(TS//STLW//SI//OC/NF)~~

CHAPTER SEVEN
DISCOVERY ISSUES RELATED TO STELLAR WIND INFORMATION ~~(TS//SI//NF)~~

In this chapter we discuss the government's statutory and judicial discovery obligations in international terrorism cases relating to Stellar Wind-derived information. Under the Stellar Wind program, the federal government collected vast amounts of information, including the content of communications and meta data about telephone and e-mail communications involving U.S. citizens and non-U.S. citizens. [redacted] (b)(1), (b)(3) [redacted] potentially triggering an obligation under the Federal Rules of Criminal Procedure and applicable case law for the government to disclose certain information to the defendant. This obligation created a tension between the need to protect the secrecy of the Stellar Wind program and the need to comply with legal disclosure requirements. ~~(TS//STLW//SI//OC/NF)~~

In this chapter, we examine the process by which the Department of Justice attempted to resolve this tension and meet its discovery obligations to criminal defendants.[403] (U)

I. Relevant Law (U)

The government's obligation to disclose certain statements made by a defendant and to disclose other information concerning a defendant in a criminal proceeding comes primarily from two sources: Federal Rule of Criminal Procedure 16 and the U.S. Supreme Court case of *Brady v. Maryland*, 373 U.S. 83 (1963). (U)

Federal Rule of Criminal Procedure 16(a)(1)(B)(i) requires the government to make various disclosures at the request of a criminal defendant. Among other things, the government must disclose "any relevant written or recorded statement by the defendant if the statement is within the government's possession, custody, or control; and the attorney for the government knows – or through due diligence could know – that the statement exists[.]" Rule 16(a)(1)(E) provides that, upon a defendant's request, the government must allow a defendant to inspect and copy papers,

[403] In our review, we did not seek to determine what the government disclosed in specific cases. Rather, we focused on the adequacy of the process that the Justice Department implemented to comply with its discovery obligations in cases that involved Stellar Wind-derived information. ~~(TS//STLW//SI//OC/NF)~~

documents, data, and other materials "if the item is within the government's possession, custody, or control" and the item is material to preparing the defense; the government intends to use the item in its case-in-chief at trial; or the item was obtained from or belongs to the defendant. (U)

Under Rule 16, a defendant's statements carry a "near presumption of relevance," and "the production of a defendant's statements has become 'practically a matter of right even without a showing of materiality.'" *United States v. Yunis*, 867 F.2d 617, 621-22, 625 & n.10 (D.C. Circuit 1989).[404] (U)

Disclosure of a defendant's statements is usually made by the government after receiving a request pursuant to Rule 16. However, even without making a Rule 16 request, a defendant has an independent right to discovery of his statements and certain other relevant information under *Brady v. Maryland*, 373 U.S. 83 (1963). *Brady* requires the government to disclose evidence in its possession favorable to the defendant and material to either guilt or punishment. Material evidence must be disclosed if it is exculpatory or if it could be used to impeach a government witness. (U)

According to an Office of Intelligence Policy and Review (OIPR) memorandum on the government's Rule 16 and *Brady* obligations

NSD b(5) - AWF

[redacted][405] (U)

However, according to the memorandum, when production of the defendant's statements or other information would reveal classified information, the government may assert a national security privilege, sometimes known as the state secrets privilege.[406] If the government asserts a colorable claim in a legal proceeding that classified information is privileged, the defendant must show that the information is not only

---

[404] See also *United States v. Scarpa*, 913 F.2d 993, 1011 (2nd Cir. 1990), citing *United States v. McElroy*, 697 F.2d 459, 464 (2nd Cir. 1982)("Rule 16 does not cover oral statements unrelated to the crime charged or completely separate from the government's trial evidence."). (U)

[405] Counsel for Intelligence Policy James Baker told us the memorandum was drafted at his request by an Assistant U.S. Attorney who had been detailed to OIPR. Baker said he requested the memorandum to refresh his understanding of the government's discovery obligations in criminal prosecutions. (U//~~FOUO~~)

[406] The state secrets privilege is a common law doctrine asserted by the United States government to protect classified information. See generally, *United States v. Reynolds*, 345 U.S. 1 (1952). (U)

relevant but material. If the defendant can show materiality, some courts balance the defendant's need for disclosure against the government's substantial interest in protecting sources and methods associated with the sensitive information. See *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988); *United States v. Smith*, 781 F.2d 1102, 1180 (4th Cir. 1985) (en banc). (U)

The government can also invoke the Classified Information Procedures Act (CIPA), 18 U.S.C. App. 3, to protect classified information in federal prosecutions. CIPA does not expand or limit a defendant's right to discovery under Rule 16; rather, CIPA allows a court, "upon a sufficient showing" to authorize the government to delete specified items of classified information from otherwise discoverable documents, substitute a summary of the information, or stipulate to relevant facts that the classified information would tend to prove. (U)

As detailed below, after aspects of the Stellar Wind program were disclosed in The New York Times and confirmed by the President in December 2005, the Justice Department invoked CIPA to prevent disclosure of the program and any program-derived information in (b)(1), (b)(3) criminal cases (b)(1), (b)(3) ~~(TS//STLW//SI//OC/NF)~~

II. Cases Raise Questions about Government's Compliance with Discovery Obligations (U)

The tension between the highly classified nature of the Stellar Wind program and the government's discovery obligations in criminal cases initially arose in (b)(1), (b)(3) ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

A. [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

The Department's awareness that Stellar Wind would have implications in criminal discovery arose in a case involving [redacted] b1, b3, b6, b7C, b7E

[redacted]

[107] [redacted] (Cont'd.) b1, b3, b6, b7C, b7E

information collected under Stellar Wind would be discoverable and, more generally, how the Stellar Wind collections might be treated in view of the government's discovery obligations in criminal prosecutions. ~~(TS//STLW//SI//OC/NF)~~

Baker said he raised these issues with Attorney General Ashcroft, FBI Director Mueller, and other Justice Department, FBI, and NSA officials. Baker stated that they concluded that a determination should first be made whether the [redacted] obtained through Stellar Wind also were captured through FISA and therefore could be produced. Baker said it turned out [redacted] had been intercepted under FISA and could be produced under that authority rather than as a result of Stellar Wind collections. Baker told the OIG that he was relieved by this outcome, but continued to be concerned about future cases. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

B. [redacted] ~~(TS//STLW//SI//OC/NF)~~

(b)(1), (b)(3), (b) (5)

[redacted] b1, b3, b6, b7C b7E

[redacted] b1, b3, b6, b7C, b7E

~~(TS//STLW//SI//OC/NF)~~

(b)(1), (b)(3), (b) (5)

[redacted]

On [redacted] Yoo orally recommended to Ashcroft that the Justice Department not disclose the Stellar Wind program intercepts to the [redacted] Yoo subsequently memorialized his advice in a memorandum. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

(b)(1), (b)(3), (b) (5)

[redacted]

b1, b3, b6, b7C, b7E

b6, b7C, b7E

[redacted]

Yoo finished his written memorandum regarding [redacted]

[redacted]

b1, b3, b6, b7C, b7E

(S//STLW//SI//OC/NF)

[redacted]

b1, b3, b6, b7C, b7E

[redacted]

b1, b3, b6, b7C, b7E

(b) (5) [411]

~~(TS//STLW//SI//OC/NF)~~

(b)(1), (b)(3), (b) (5)

b1, b3, b6, b7C, b7E

~~(TS//STLW//SI//OC/NF)~~

As a final point, Yoo wrote, (b) (5)

~~(TS//STLW//SI//OC/NF)~~

b1, b3, b6, b7C, b7E

(b)(1), (b)(3), (b) (5)

[411]

(b)(1), (b)(3), (b) (5)

b1, b3, b6, b7C, b7E

[412] At the time Yoo wrote the (b)(1), (b)(3) memorandum, he, Baker, and Ashcroft were the only non-FBI Justice Department officials read into the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

[413]

(b)(1), (b)(3), (b) (5)

b1, b3, b7E

[414]

(b) (5), (b)(1), (b)(3)

(Cont'd.)

b1, b3,b7E

(b)(1), (b)(3), (b)(5)

b1, b3, b6, b7C, b7E

In another internal Justice Department review of his actions, Yoo has acknowledged that he is not well versed in criminal law. During an interview with the Department's Office of Professional Responsibility (OPR) in connection with its investigation concerning his legal opinions in support of a detainee interrogation program, Yoo stated that "criminal prosecution process in the Department was not my specialty," and "criminal law was not my area."[415] ~~(TS//SI//OC/NF)~~

III. Criminal Division Examines Discovery Issues (U)

Following (b)(1), (b)(3) the Justice Department's Criminal Division was tasked with developing procedures for handling Rule 16 disclosure issues because the issues fell within its area of expertise. As a result, in (b)(1), (b)(3) Patrick Rowan, a senior counsel in the Criminal Division, was read into the program to deal with Stellar Wind-related discovery issues. Rowan's supervisor, Criminal Division Assistant Attorney General Christopher Wray, was also read into the program at the same time.

b1, b3, b6, b7C, b7E

(b)(5)

b1, b3, b6, b7C, b7E

[415] The OPR investigation concerned a Top Secret compartmented program relating to detainee interrogations. Yoo drafted legal opinions for this program while in the Office of Legal Counsel. However, as discussed in Chapter Four, in contrast with the Stellar Wind program at least four other OLC attorneys assisted Yoo with drafting the legal memoranda. Yoo was also able to consult with Criminal Division attorneys and the client agency on this matter. ~~(TS//STLW//SI//OC/NF)~~

Wray and Rowan were the first Department attorneys with Criminal Division-level responsibility for terrorism prosecutions to be read into the program. ~~(TS//STLW//SI//OC/NF)~~

Wray told the OIG that after his and Rowan's read-in, they "were kind of left on our own." He said that no one directed him or Rowan to continue studying the Rule 16 issues or the government's *Brady* obligations in connection with international terrorism prosecutions, nor did anyone tell them to develop any judgments or opinions on the subject. (U)

Wray told us that at some point after his read-in he may have read Yoo's (b)(1), (b)(3) memorandum on the Department's discovery obligations in [redacted] and he instructed Rowan to review the memorandum. Rowan told us that he was familiar with Yoo's memorandum, but stated that he could not recall whether the purpose of Yoo's memorandum was to lay out in general the pertinent legal issues or to document how [redacted] in particular was to be handled. Rowan told us that he did not recall having any problems with the conclusions Yoo reached. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

A. The "Informal Process" for Treating Discovery Issues in International Terrorism Cases (U)

During his OIG interview, Rowan described the processes at the Department prior to the December 2005 disclosure of aspects of the Stellar Wind program in The New York Times to address discovery obligations with respect to Stellar Wind-derived information. He said that the NSA was generally aware of the Justice Department's international terrorism criminal cases, at least in part due to NSA's ongoing contacts with Patrick Philbin and others in the Department. According to Rowan, the NSA's general awareness of the Department's international terrorism docket amounted to an "informal process" for spotting cases that may present discovery issues. Rowan stated that prosecutors in U.S. Attorney's Offices typically would request the NSA to perform "prudential searches" of its databases for any relevant information concerning their prosecutions, including for discovery purposes, although this did not happen in every international terrorism case. Rowan stated that if the NSA located any responsive but classified information, it would be expected to notify senior Justice Department officials with the requisite clearances about the information. Rowan said he was confident that if *Brady* information were known to the NSA, it would be brought to the attention of the Department and steps would have been taken to dismiss the case or otherwise ensure the program was not disclosed. ~~(TS//STLW//SI//OC/NF)~~

In addition to these routine communications between Department prosecutors and the NSA in criminal prosecutions, Rowan described other

measures that were in place to keep Stellar Wind-derived information out of the criminal prosecution process. He stated that the FBI had "walled off" any evidence it collected from inclusion in criminal cases by tipping out Stellar Wind-derived information under [redacted] with a caveat that the information in the tipper was "for lead purposes only." Rowan noted that OIPR also had in place a scrubbing process to delete program-derived information from FISA applications. Rowan expressed confidence that these mechanisms ensured that no program information was used in international terrorism prosecutions.[416] Finally, Rowan stated that the FBI is "very quick to get FISAs up," thereby minimizing the likelihood that the NSA's Stellar Wind database would be the sole repository of *Brady* material. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

B. (b) (5) [redacted] Memorandum Analyzing Discovery Issues Raised by the Stellar Wind Program ~~(TS//STLW//SI//OC/NF)~~

At the direction of Assistant Attorney General Wray, Rowan memorialized his research regarding these discovery issues in a memorandum entitled (b) (5) [redacted] Rowan said he worked on the memorandum largely alone, consulting occasionally with Wray. Rowan said it was very difficult to work on the matter because of the secrecy surrounding the program and the other demands of his job.[417] ~~(TS//STLW//SI//OC/NF)~~

In his (b) (5) [redacted] memorandum, (b) (5) [redacted]

[416] As discussed in Chapter Six, the caveats were intended to exclude at the outset any Stellar Wind-derived information from FISA applications and other criminal pleadings. The scrubbing process acts as a second check against including this information in FISA applications. However, neither the caveats nor the scrubbing process relieved the government of its obligations under *Brady* to disclose evidence in the government's possession favorable to the defendant and material to either guilt or punishment. ~~(TS//STLW//SI//OC/NF)~~

[417] The memorandum noted, "Because there were no additional attorneys within the Criminal Division who were read into the program (and very few in the Department generally), we have been unable to assign work to others or to fully consult with others within the Division." ~~(TS//SI//NF)~~

(b) (5) [redacted] b1, b3, b6, b7C, b7E

(b) (5)

[redacted]

b1, b3, b7E

(b) (5)

[redacted]

b1, b3, b7E

Rowan's memorandum also referred to guidance in the United States Attorney's Manual (USAM). For cases in which the Intelligence Community had no active involvement in the criminal investigation, the USAM stated that there are two circumstances in which the prosecutor must conduct a "suitable search" of Intelligence Community files: (1) where the prosecutor has "direct or reliable knowledge" that the Intelligence Community

b1, b3, b6, b7C, b7E

(b) (5)

[redacted]

possesses potential *Brady* or other discovery material; or, (2) in the absence of such knowledge, where "there nonetheless exists any reliable indication suggesting" that the Intelligence Community possesses such material. USAM, Criminal Resources Manual § 2052 (2002). The USAM stated that, as a general rule, a prosecutor should not seek access to Intelligence Community files unless there is an affirmative obligation to do so. However, it noted that certain types of cases, including terrorism prosecutions, fall outside this general rule. In such cases, the USAM advised that the prosecutor should conduct a "prudential search." Id. ~~(TS//STLW//SI//OC/NF)~~

Rowan wrote that the practice in several sections within the Criminal Division was to "generally go beyond both the legal obligations outlined [in his memorandum] and the general rule outlined in the USAM, initiating searches out of prudence, rather than a legal obligation." For instance, Rowan reported that the practice of the Criminal Division's Counterespionage Section (CES) was to search Intelligence Community files in almost every case, even in instances in which the Intelligence Community had no involvement in the investigation or prosecution [redacted] (b) (5) [redacted][420] ~~(TS//STLW//SI//OC/NF)~~

(b) (5) [redacted][421] In cases involving the NSA, the typical practice

---

[420] The OIG interviewed John Dion, the Chief of CES, which became part of the National Security Division in 2006. [redacted] (b) (5) [redacted] Dion stated that such searches are conducted in cases in which there is likely to be intelligence collection concerning the defendant as "suggested by the facts of the matter." He added that the searches were requested for a variety of reasons, including for purposes of meeting discovery obligations. Dion said that searches also were requested to determine whether the defendant has a "relationship" with an intelligence agency. He noted that CES does not request prudential searches as a matter of course to avoid making spurious requests. ~~(S//NF)~~

[421] [redacted] (b) (5) [redacted] Dion said CES was a proponent of the position that line prosecutors with whom CES co-prosecutes cases should have the same knowledge as CES concerning the "national security equities" involved in each case. Dion said this arrangement also allows for the AUSA, who is often the prosecutor most familiar with the case and the jurisdictional practices, to review any Intelligence Community material for Rule 16 and *Brady* purposes. Dion acknowledged the limitations to this arrangement concerning strictly compartmented programs such as Stellar Wind, where the NSA understandably would be reluctant to read in line prosecutors for the limited purpose of screening defense discovery requests. ~~(TS//STLW//SI//OC/NF)~~

was for the CES attorney to use the provisions of CIPA to prevent disclosure of sensitive material. Rowan noted that other sections within the Criminal Division also relied on CIPA to protect Intelligence Community files found during searches. ~~(TS//SI//OC/NF)~~

(b) (5)

(b) (5)

Thus, although Rowan's memorandum did not contain a proposal for handling discovery requests in cases involving Stellar Wind, it identified key legal issues that would have to be addressed as a part of any such proposal.

(b) (5)

~~(TS//STLW//SI//OC/NF)~~

---

422 When Rowan became principally responsible for coordinating the Department's responses to defense discovery requests as a Deputy Assistant Attorney General in the (Cont'd.)

C. Office of Legal Counsel and Discovery Issue (U)

Shortly before Rowan finished his memorandum in (b) (5) OLC Principal Deputy Assistant Attorney General Steve Bradbury became the acting head of OLC. Bradbury told us that he recalled having some discussion with Rowan about how discovery matters should be handled in connection with the Stellar Wind program. Bradbury said that John Eisenberg, later a Deputy in OLC, also may have discussed the matter with Rowan. Bradbury stated that he did not believe that OLC followed up on Rowan's request that it continue researching these issues. ~~(TS//STLW//SI//OC/NF)~~

Eisenberg told us that he discussed the Rule 16 issue with Rowan at some point, but did not recall whether they discussed the *Brady* issue. He recalled discussing Yoo's (b)(1), (b)(3) memorandum with Rowan and said he believes the Justice Department took the position that the Yoo memorandum was correct, at least with respect to Yoo's legal analysis in (b)(1), (b)(3) ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

When we showed Eisenberg a copy of Rowan's (b) (5) memorandum, Eisenberg stated that he had not previously seen it. Eisenberg told us that OLC would not typically be responsible for addressing the discovery issues presented in Rowan's memorandum and that he was not aware of any OLC opinion on the subject other than Yoo's memorandum. Eisenberg also said he was not aware of any formal procedures for handling Rule 16 disclosure requests or the government's affirmative *Brady* obligations other than the *ex parte* in camera motions practice pursued by the National Security Division, discussed below. ~~(TS//STLW//SI//OC/NF)~~

CES Chief Dion agreed that OLC would not be the appropriate entity to review discovery procedures in the context of Stellar Wind, in part because OLC attorneys generally do not have criminal litigation expertise. Dion suggested that if the Department were to develop procedures for handling discovery of Intelligence Community files, it should be done by the Department's National Security Division in coordination with United States Attorneys' Offices, and it should be binding only on those two entities. Rowan, while generally agreeing with Dion, told the OIG that he believed the OLC appropriately could have analyzed the legal issue of what impact a

National Security Division in 2006. (b) (5) The results of these searches were produced to the courts *ex parte*, in camera, pursuant to CIPA. ~~(TS//STLW//SI//OC/NF)~~

guilty plea would have on the government's *Brady* obligations. ~~(TS//STLW//SI//OC/NF)~~

Wray also told us that there was no organized Departmental effort to establish formal procedures for reviewing international terrorism prosecutions to comply with Rule 16 disclosure requests and *Brady* obligations. He said "the thinking was" that the Rowan memorandum was the "first step" toward devising "some kind of systematized process" for such reviews. However, we found no indication that OLC followed up on Rowan's request to further study these discovery issues with any kind of written product. ~~(TS//STLW//SI//OC/NF)~~

IV. Use of the Classified Information Procedures Act (CIPA) to Respond to Discovery Requests (U)

After publication of The New York Times articles in December 2005, the Justice Department received numerous discovery requests in connection with international terrorism prosecutions throughout the country. After these articles, additional officials in the Criminal Division were read into the Stellar Wind program, including the new Assistant Attorney General Alice Fisher and other senior officials, both to assist with the Criminal Division's investigation into the leak of information to The New York Times and to handle the discovery requests following the public confirmation of the program by the President and other Administration officials in December 2005.[423] After the National Security Division was created in September 2006, it assumed much of the responsibility for handling the responses to discovery requests. ~~(TS//STLW//SI//OC/NF)~~

Typically, the defense motions sought to compel the government to produce information concerning a defendant that had been derived from the "Terrorist Surveillance Program," the term sometimes used by the government to refer to what the President confirmed after publication of The New York Times articles. The government responded to the discovery requests by filing *ex parte* in camera responses requesting to "delete items" from material to be produced in discovery pursuant to CIPA. ~~(S//NF)~~

In the following sections we provide a brief overview of CIPA and its use in international terrorism cases potentially involving Stellar Wind-derived intelligence. ~~(TS//STLW//SI//OC/NF)~~

[redacted]

(b)(3)

A. Overview of CIPA (U)

The Classified Information Procedures Act, 18 U.S.C. App. 3, was enacted in 1980 to provide procedures for protecting classified information in federal criminal prosecutions. When a party to a criminal proceeding notifies the court that classified information will be used in the course of the proceeding, CIPA requires the court to initiate procedures to "determine the use, relevance, or admissibility of the classified information that would otherwise be made during the trial or pretrial proceeding." 18 U.S.C. App. 3 § 6(a). Where the government holds the classified information, it may bring the matter before the court *ex parte*, but it also must provide notice to the defense that classified information is at issue. Id. at § 6(b)(1). (U)

Protective procedures generally are established through a CIPA hearing with both parties present. The hearing may be conducted in camera if the government certifies that an in camera hearing is necessary to protect the classified information. Id. at § 6(a). Typically, the government seeks an order to protect against the disclosure of any classified information to the defense. The government may also seek to withhold production of the classified information in one of three ways: (1) deletion of the classified items from the material disclosed to the defendant, (2) summarization of the classified information, or (3) admission of certain facts that the classified information would tend to prove. Id. at § 4. Based on the OIG's review of CIPA filings related to the Stellar Wind program, the government has only used option 1 (deleting classified items from material to be disclosed to the defendant) in response to defense motions for Stellar Wind information. ~~(TS//STLW//SI//OC/NF)~~

To prevent the disclosure of classified information, the government may make an *ex parte* showing to the court. To do so the government must submit "an affidavit of the Attorney General certifying that disclosure of classified information would cause identifiable damage to the national security of the United States and explaining the basis for the classification of such information." Id. at § 6(c)(2). If the court decides that the defendant's right to access to the evidence outweighs the government's national security interests, the government can choose to dismiss the indictment rather than make a disclosure. *United States v. Moussaoui*, 382 F.3d 453, 466 n. 18, 474-76 (4th Cir. 2004). (U)

B. Use of CIPA in International Terrorism Prosecutions Alleged to Involve Stellar Wind-Derived Information ~~(TS//STLW//SI//OC/NF)~~

We reviewed the CIPA pleadings files maintained in the National Security Division relating to the Stellar Wind program. In almost every instance, the CIPA litigation was handled by the National Security Division

without the involvement of the line prosecutors in the U.S. Attorney's Offices who handled the underlying prosecutions but who were not read into the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

(b)(1), (b)(3)

Rowan, who became the National Security Division Acting Assistant Attorney General in April 2008 and was confirmed as the Assistant Attorney General in September 2008, told us that

(b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~

The scope and nature of the defense motions initiating the CIPA litigation varied, depending on the procedural posture of the case. For instance, some defense motions sought to compel discovery of NSA surveillance information, while others sought to suppress all government evidence and, in the alternative, have the government's case dismissed on the theory that illegal electronic surveillance caused the government to initiate its criminal investigation in the first instance.

(b)(1), (b)(3)

~~(TS//STLW//SI//OC/NF)~~

Regardless of the varying procedural posture of the cases and the scope and nature of the defense motions, the government responses we examined were fairly uniform, consisting of a motion to delete items from discovery, a legal memorandum in support of the motion, declarations from senior FBI and NSA officials, and a proposed order. ~~(TS//STLW//SI//OC/NF)~~

(b)(3)

~~(TS//STLW//SI//OC/NF)~~

The government's CIPA submissions asserted that the information at issue in the discovery litigation was classified and subject to the national security privilege as codified in CIPA. They generally described the types of information its searches of intelligence databases (including Stellar Wind) might reveal. (b)(3)

(b)(3), (b)(1)

[redacted]

4,21

(b)(1), (b)(3)

[redacted]

(b)(1), (b)(3) [redacted] [425]

The government's responses we reviewed uniformly stated that information in the NSA's intelligence reports had not been or would not be used as evidence, and that there was no causal connection between the information in the reports and any evidence used or to be used at trial, or was too attenuated from the evidence to be discoverable. The government argued that because the facts concerning the NSA's reporting would not aid the defense, the court need not explore the sources and methods used to acquire the information. The submissions also argued that the information collected by the NSA was not included in the government's FISA application, and therefore was too attenuated from the trial evidence to merit a review of the means by which the intelligence information was gathered. The government asserted that the "causal connection" between discovery of the derivative evidence and the alleged illegal search "may have become so attenuated as to dissipate the taint."[426] It is important to note that the government did not argue in the CIPA responses we reviewed that [redacted] (b) (5), (b)(1), (b)(3) [redacted] ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

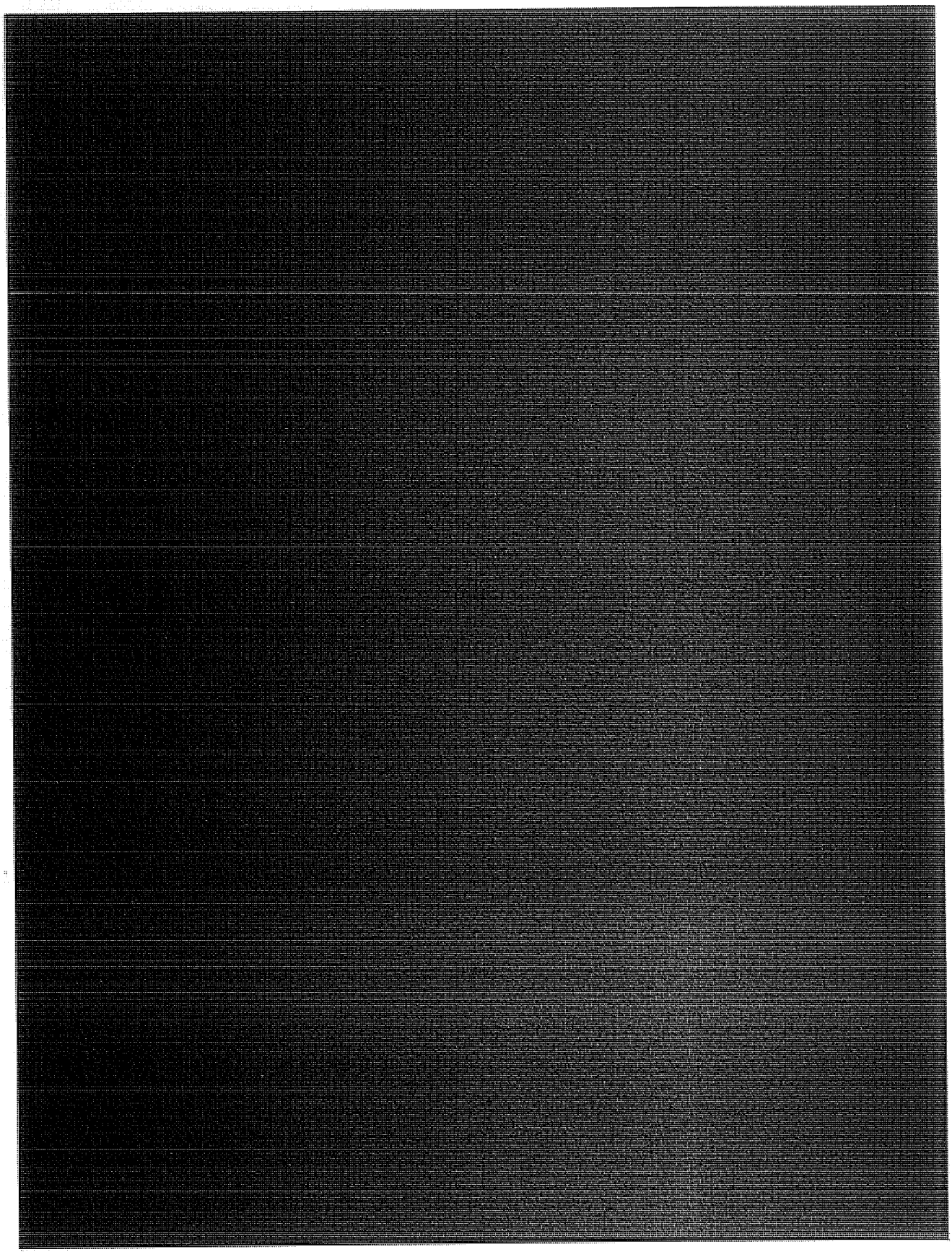
C. Government Arguments in Specific Cases (U)

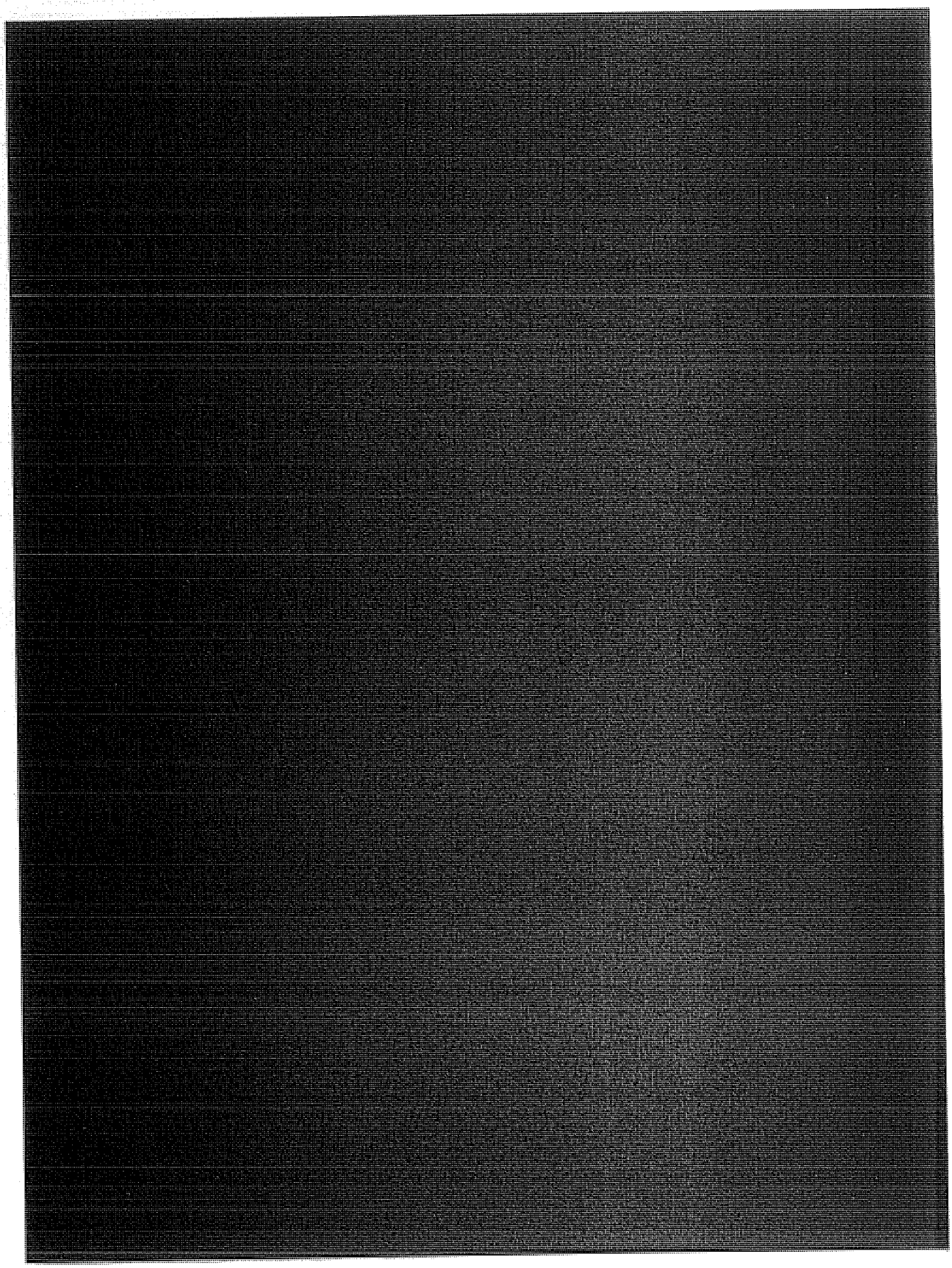
In this section we describe [redacted] cases that illustrate the arguments made by the government in CIPA litigation with respect to defendant's requests for discovery of Stellar Wind-derived information. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

[redacted]

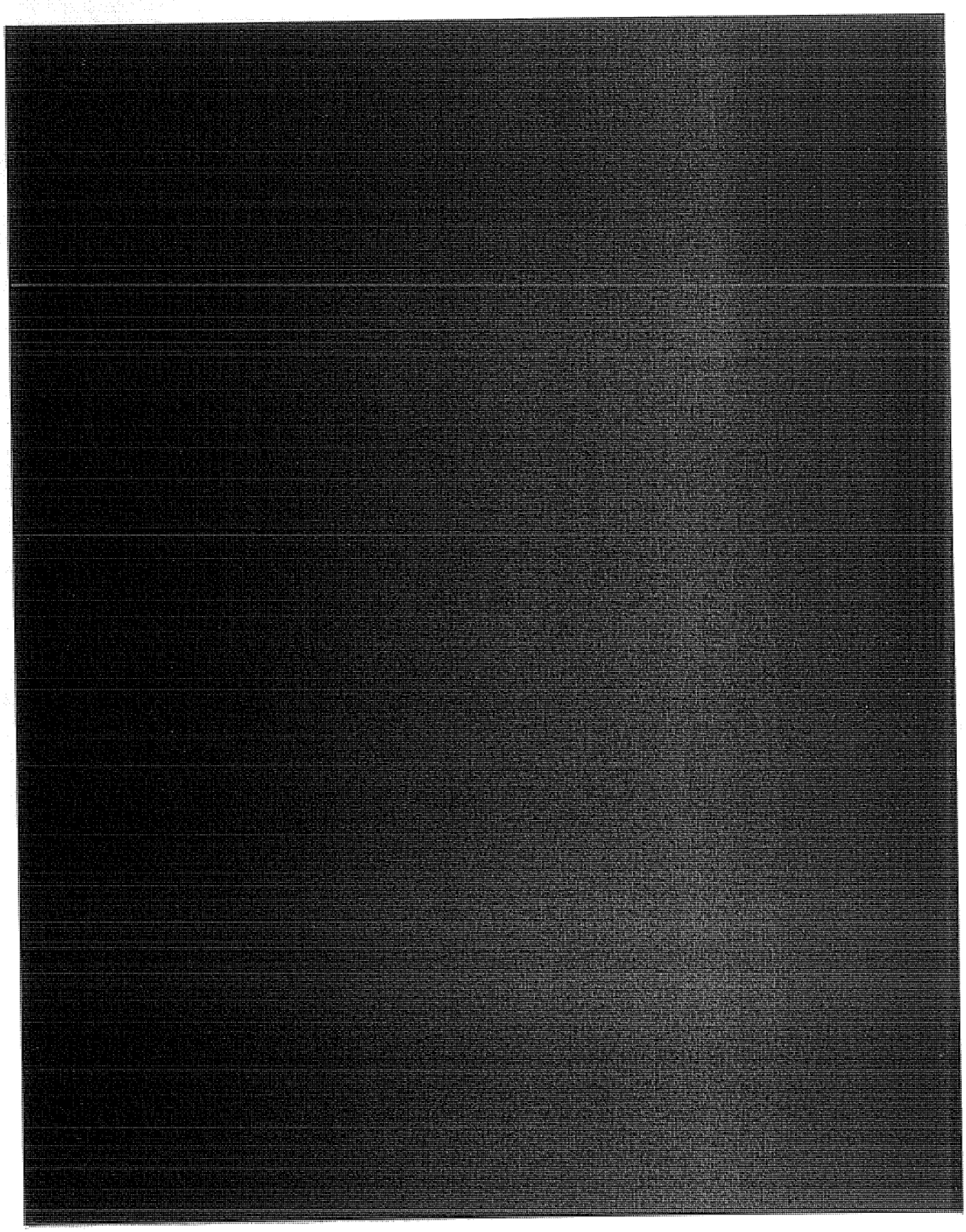
[425] In several instances, the Stellar Wind information was disseminated within the FBI after the FBI already had obtained a FISA order to conduct electronic surveillance of the defendant, thus allowing the government to argue that the NSA reporting played no role in its acquisition of the evidence used or planned to be used against the defendant. ~~(TS//STLW//SI//OC/NF)~~

[426] *Nardone v. United States*, 308 U.S. 338, 341 (1939). The government also argued in its submissions that suppressing its evidence would not serve any deterrence purpose. The government argued that the NSA acquires, processes, and disseminates intelligence not to produce criminal prosecutions, but to protect the national security. It asserted that any suppression of evidence would therefore frustrate a criminal prosecution and create an incentive for the intelligence community not to share information with law enforcement, thereby harming national security. ~~(TS//SI//OC/NF)~~

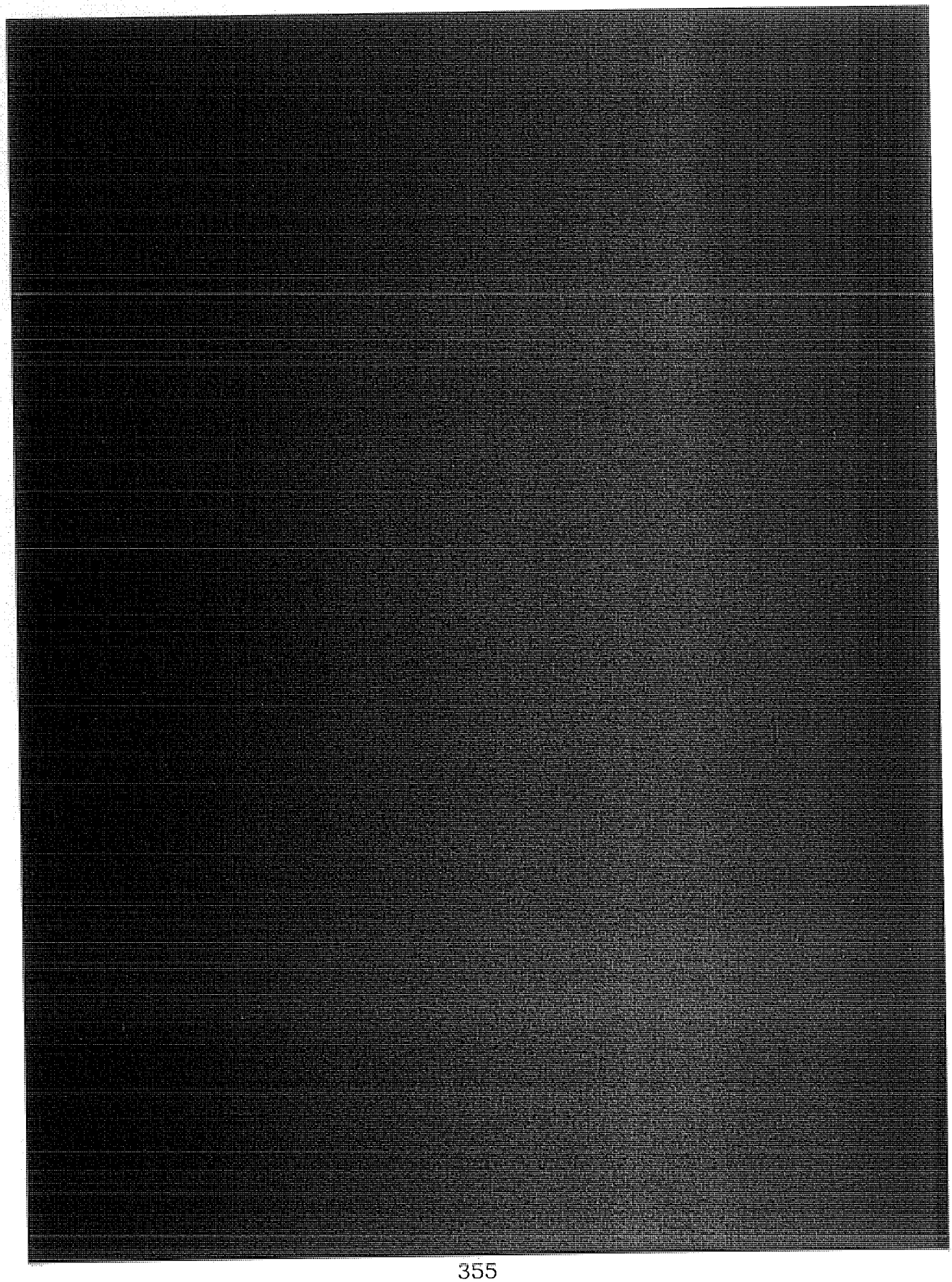




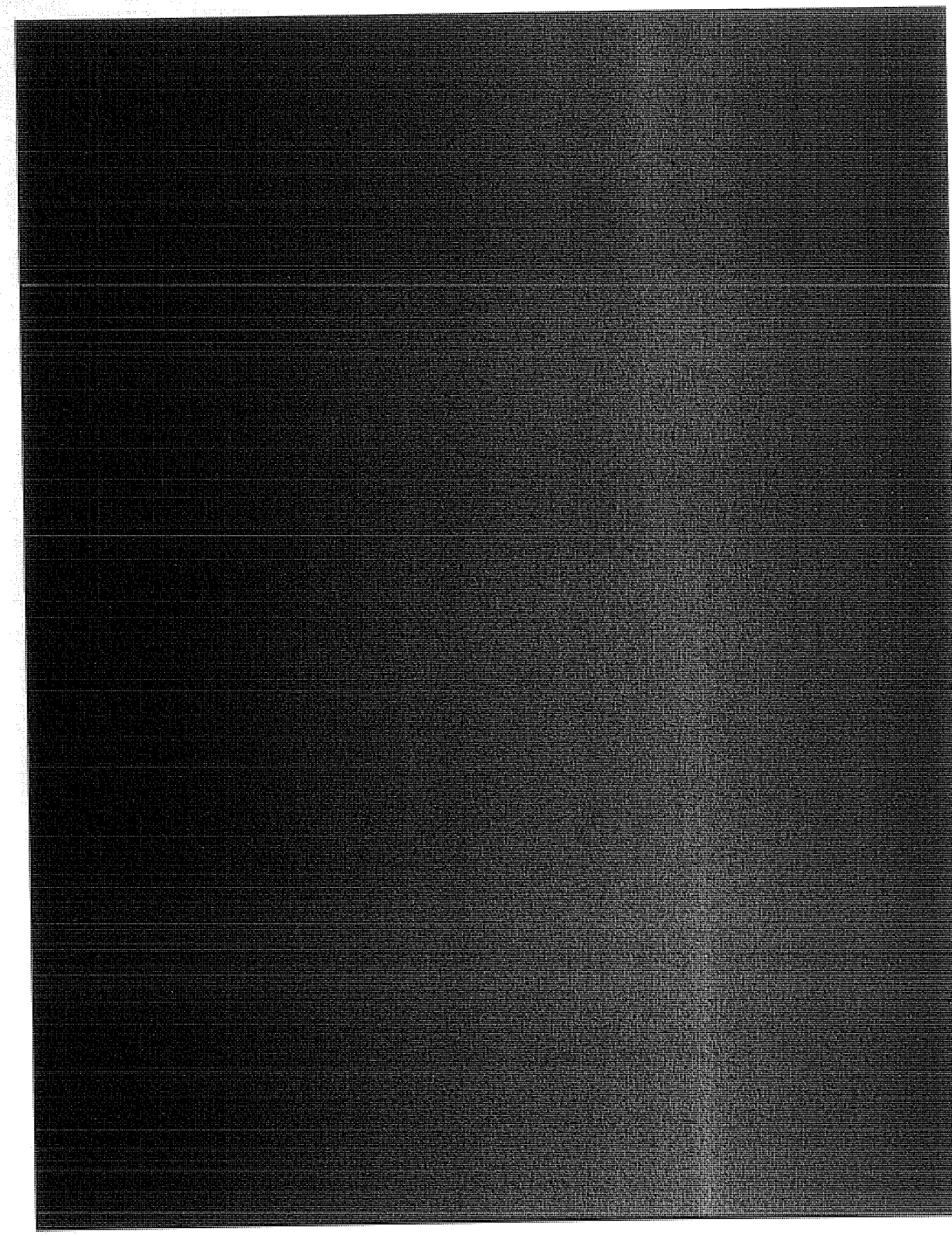
b1, b3, b6,
b7C, b7E



b1, b3, b6, b7C, b7E



b1, b3, b6, b7C, b7E



[redacted]

V. OIG ANALYSIS (U)

We found that the Department made little effort to understand and comply with its discovery obligations in connection with Stellar Wind-derived information for the first several years of the program. The Department's limited initial effort was also hampered by the limited number of attorneys who were read into the program. As a result, OLC attorney John Yoo alone initially analyzed the government's discovery obligations in one early case, and he produced a legal analysis that was based on an incorrect understanding of the facts of the case to which it applied. When other attorneys from the Department's Criminal Division eventually were read into the program, (b) (5) [redacted] At that point, the Department eventually took steps to address [redacted] its discovery obligations. However, in our view, those steps are not complete and do not fully ensure that the government has met its discovery obligations regarding information obtained through the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

As described in this chapter, in 2002 the Department first recognized that the Stellar Wind program could have implications for discovery obligations in terrorism cases. OIPR Counsel Baker raised with Department

[redacted]

b1, b3, b6, b7C, b7E

and FBI officials the question of how the government would meet its discovery obligations regarding Stellar Wind information. Despite awareness of this issue, the Department took no action at this time to ensure that it was in compliance with Rule 16 or *Brady* with respect to Stellar Wind-derived information. We believe that at this point senior Department officials were on notice that, at a minimum, the discovery issue merited attention. However, no concrete action was taken until early [redacted] in the context of [redacted] when the Department had to address how to handle Stellar Wind information that was not also obtained under FISA and that could be material to the defense under Rule 16. This issue was assigned to Yoo, who concluded [redacted]

b1, b3, b6, b7C, b7E

(b) (5)

[redacted]

~~(TS//STLW//SI//OC/NF)~~

(b) (5), (b)(1), (b)(3)

[redacted]

b1, b3, b6, b7C, b7E

As with other aspects of the Stellar Wind program, we believe the error in Yoo's legal analysis may have resulted in part from the failure to subject his memorandum to typical OLC and Department review and scrutiny. Because other Department attorneys were not read into the Stellar Wind program, the risk that the Department would produce a factually flawed and inadequate legal analysis of these important discovery issues was escalated. As we concluded in Chapters Three and Four, we believe the lack of sufficient legal resources at the Department during this early phase of the Stellar Wind program hampered its legal analysis of important issues related to the program. We believe that Yoo's (b)(1), (b)(3) memorandum is one more manifestation of this problem.

b1, b3, b6, b7C, b7E

~~(TS//STLW//SI//OC/NF)~~

In July 2004, Patrick Rowan, a senior counsel in the Criminal Division, was read into the program and conducted a more systemic analysis of the Department's discovery obligations with regard to Stellar Wind information. [redacted]

(b) (5)

[redacted]

(b) (5) [redacted] (TS//STLW//SI//OC/NF)

(b) (5) [redacted]

With his memorandum, Rowan initiated a request that the issue be further examined by OLC. ~~(TS//SI//NF)~~

However, other than in informal discussions with Rowan concerning Yoo's [redacted] memorandum, OLC did not further examine these issues or follow up on Rowan's recommendation. While we recognize that OLC was not responsible for developing litigative strategy on this issue, we believe that OLC or another appropriate Department component should have provided guidance on this important legal issue. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b6, b7C, b7E

We recommend that the Department conduct a comprehensive legal assessment of the important issues (b) (5) that still remain unresolved (b) (5) [redacted] the legal ramifications of a guilty plea on the government's disclosure obligations under Rule 16 and in particular *Brady*. We believe the Department should carefully consider whether it must re-examine past cases to see whether potentially discoverable but undisclosed Rule 16 or *Brady* material was collected by the NSA, and take appropriate steps to ensure that it has complied with its discovery obligations in such cases. ~~(TS//SI//NF)~~

The Department took steps to respond, on a case-by-case basis, to discovery motions (b)(1), (b)(3) [redacted]

However, the Department's handling of these motions did not require the Department to identify the potentially discoverable information derived under the Stellar Wind program that may exist in other cases. We recommend that the Department, in coordination with the NSA, develop and implement a procedure for identifying Stellar Wind-derived information that may be associated with international terrorism cases, currently pending or likely to be brought in the future, and to evaluate such information in light of the government's discovery obligations under Rule 16 and Brady. ~~(TS//STLW//SI//OC/NF)~~

CHAPTER EIGHT
PUBLIC STATEMENTS ABOUT THE SURVEILLANCE PROGRAM (U)

This chapter examines Attorney General Alberto Gonzales's testimony and public statements related to the Stellar Wind program. Aspects of this program were first disclosed publicly in a series of articles in The New York Times in December 2005. In response, the President publicly confirmed a portion of the Stellar Wind program – the interception of the content of international communications of people reasonably believed to have links to al Qaeda and related organizations. Subsequently, Attorney General Gonzales was questioned about the program in two hearings before the Senate Judiciary Committee in February 2006 and July 2007. ~~(S//NF)~~

In between those two hearings, former Deputy Attorney General James Comey testified before the Senate Judiciary Committee about the dispute between the Department and the White House concerning the program. Gonzales's and Comey's differing congressional testimony led to allegations that Gonzales had made misleading statements to Congress about the dispute and the program itself.[434] (U)

In this chapter, we examine whether Attorney General Gonzales made false, inaccurate, or misleading statements related to the Stellar Wind program. (U//~~FOUO~~)

I. Summary of the Dispute about the Program (U)

As described in detail in Chapters Three and Four, the Stellar Wind program is best understood as consisting of three types of collections, informally referred to as "baskets." Basket 1 related to the collection of e-mail and telephone content. Initially, the Stellar Wind program collected e-mail and telephone content when probable cause existed to believe one of the parties to the call or e-mail was outside the United States and at least one of the communicants was a member of an international terrorist group.

[434] For example, Senator Arlen Specter stated at a Senate hearing on July 24, 2007, that he did not find Attorney General Gonzales's testimony to be credible and suggested to the Attorney General that he "review this transcript very, very carefully." After this hearing Senate Judiciary Committee Chairman Patrick Leahy sent a letter to the OIG, dated August 16, 2007, asking the OIG to review Gonzales's statements to determine whether they were intentionally false, misleading, or inappropriate. Gonzales testified several times before the Senate and House Judiciary and Intelligence Committees about the program. In this chapter, we focus on his February 2006 and July 2007 testimony in which he discussed the events of March 2004. (U)

Basket 2 involved bulk collection of telephony meta data, and basket 3 involved bulk collection of e-mail meta data. (~~TS//STLW//SI//OC/NF~~)

These collections were authorized by a Presidential Authorization that was re-issued at approximately 30 to 45-day intervals. Each Authorization was certified as to form and legality by the Attorney General. The Attorney General's certifications were initially supported by legal opinions from OLC attorney John Yoo affirming the legality of the program. (~~TS//STLW//SI//OC/NF~~)

As discussed in Chapter Four, after Jack Goldsmith was confirmed as Assistant Attorney General for OLC in October 2003, he, along with Associate Deputy Attorney General Patrick Philbin, conducted an analysis of the legal basis underlying each basket in the Stellar Wind program. As a result of this review, he, Philbin, and recently confirmed Deputy Attorney General Comey concluded that they could find no legal support for several aspects of the existing program.

[redacted]

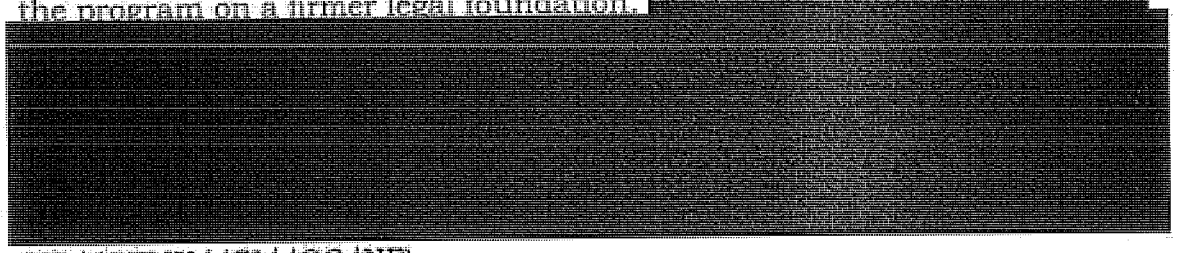
(~~TS//STLW//SI//OC/NF~~)

[redacted]

In early March 2004, the dispute between the Department and the White House over the Department's revised legal analysis of the Stellar Wind program came to a head. Deputy Attorney General Comey, who assumed the duties of the Attorney General when Attorney General Ashcroft was hospitalized, informed the White House that the Department could not recertify the program. This dispute culminated in the unsuccessful attempt by then-White House Counsel Gonzales and White House Chief of Staff Andrew Card to get Attorney General Ashcroft to overrule Comey and recertify the program while he was in the hospital. When Ashcroft refused to certify the program and said that Comey was acting as the Attorney General, not him, the President reauthorized the program without the

Attorney General's certification. Instead Gonzales, as White House Counsel, recertified the program. ~~(TS//SI//NF)~~

After the White House's actions to continue the program without Justice Department certification, Deputy Attorney General Comey, FBI Director Mueller, and many other senior Department officials considered resigning. When the President learned of this, he directed that the Department work with other involved agencies and the White House to place the program on a firmer legal foundation.



~~(TS//STLW//SI//OC/NF)~~

II. The New York Times Articles and President Bush's Confirmation Regarding NSA Activities (U)

In 2004, aspects of the Stellar Wind program were disclosed to two reporters for The New York Times. The reporters, James Risen and Eric Lichtblau, sought to publish an article about the program in late 2004. However, after a series of meetings with Administration officials who argued that publication of the story would harm the national security, The New York Times agreed to delay publishing the story. ~~(S//NF)~~

The New York Times eventually published a series of articles about the program on December 16 through 19, 2005. According to one of the reporters, the Times decided to publish the articles at least in part because the newspaper learned of serious concerns about the legality of the program that had "reached the highest levels of the Bush Administration."[435] (U)

The first article, on December 16, 2005, was entitled, "Bush Lets U.S. Spy on Callers Without Courts." This article stated that "Months after the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying, according to government officials." The article described in broad terms the content collection aspect of the NSA program (basket 1), stating that according to officials the NSA has "monitored the international telephone calls of hundreds, perhaps

---

435 See Eric Lichtblau, *Bush's Law* (2008), p. 203. (U)

thousands, of people inside the United States without warrants over the past three years in an effort to track possible 'dirty numbers' linked to al Qaeda." The article stated that the NSA continued to seek warrants to monitor purely domestic communications. ~~(TS//STLW//SI//OC/NF)~~

The article asserted that "reservations about aspects of the program" had also been expressed by Senator Jay Rockefeller (the Vice Chair of the Senate Select Committee on Intelligence) and a judge who presided over the FISA Court. The article added, "Some of the questions about the [NSA's] new powers led the administration to temporarily suspend the operation last year and impose more restrictions, officials said." The article also stated that "In mid-2004, concerns about the program expressed by national security officials, government lawyers and a judge prompted the Bush administration to suspend elements of the program and revamp it." However, the article incorrectly tied this suspension of the program to Judge Colleen Kollar-Kotelly's concerns that information gained from the program was also being used to seek FISA orders, rather than to the March 2004 dispute between Department officials and the White House about the legality of aspects of the program. ~~(TS//SI//NF)~~

On December 17, 2005, the day after The New York Times published the first article, President Bush publicly acknowledged the portion of the NSA program that was described in the article. President Bush described in broad terms these NSA electronic surveillance activities, stating:

> In the weeks following the terrorist attacks on our nation, I authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations. Before we intercept these communications, the government must have information that establishes a clear link to these terrorist networks.
>
> This is a highly classified program that is crucial to our national security. Its purpose is to detect and prevent terrorist attacks against the United States, our friends and allies. Yesterday the existence of this secret program was revealed in media reports, after being improperly provided to news organizations. As a result, our enemies have learned information they should not have, and the unauthorized disclosure of this effort damages our national security and puts our citizens at risk. Revealing classified information is illegal, alerts our enemies, and endangers our country . . . .
>
> The activities I authorized are reviewed approximately every 45 days. Each review is based on a fresh intelligence assessment of terrorist threats to the continuity of our government and the

threat of catastrophic damage to our homeland. During each assessment, previous activities under the authorization are reviewed. The review includes approval by our nation's top legal officials, including the Attorney General and the Counsel to the President. I have reauthorized the program more than 30 times since the September 11th attacks, and I intend to do so for as long as our nation faces a continuing threat from al Qaeda and related groups.[436] (U)

III. Other Administration Statements (U)

On January 19, 2006, the Justice Department issued a document, informally referred to as a "White Paper," entitled "Legal Authorities Supporting the Activities of the National Security Agency Described by the President." The 42-page document addressed in an unclassified form the legal basis for the collection activities that were described in the December 16, 2005, New York Times article and other media reports and confirmed by President Bush. The White Paper stated that the President acknowledged that "he has authorized the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or other related terrorist organizations." (U)

The White Paper reiterated the legal theory advanced by the Department in Goldsmith's May 2004 memorandum about the revised NSA program, which concluded that the September 18, 2001, Congressional Authorization for the Use of Military Force authorized the President to employ "warrantless communications intelligence targeted at the enemy," a fundamental incident of the use of military force, pursuant to the President's Article II Commander-in-Chief powers. The White Paper also argued that the NSA's activities were consistent with FISA, as confirmed and supplemented by the AUMF. ~~(TS//SI//NF)~~

On January 22, 2006, the White House also issued a press release and memorandum to counter criticism of the NSA program by members of Congress. The press release was entitled "Setting the Record Straight: Democrats Continue to Attack the Terrorist Surveillance Program." This document was the first time we found any official use of the term "Terrorist Surveillance Program" to apply to the NSA program or aspects of the program.[437] ~~(S//NF)~~

---

[436] The full text of President Bush's December 17, 2005, radio address can be found at http://www.whitehouse.gov/news/releases/2005/12/print/20051217.html. (U)

[437] See http://www.whitehouse.gov/news/releases/2006/01/200060122.html. We found that the term was used in the media prior to this time. The first published reference (Cont'd.)

The following day, on January 23, 2006, President Bush referred to the "terrorist surveillance program" during a speech at Kansas State University:

> Let me talk about one other program . . . something that you've been reading about in the news lately. It's what I would call a terrorist surveillance program. (U)

In the speech, President Bush described the program as the interception "of certain communications emanating between somebody inside the United States and outside the United States; and one of the numbers would be reasonably suspected to be an al Qaeda link or affiliate." (U)

On January 24, 2006, Attorney General Gonzales delivered a speech at the Georgetown University Law Center which, according to his prepared remarks, began by stating that his remarks "speak only to those activities confirmed publicly by the President, and not to purported activities described in press reports." Gonzales referred to the program throughout his speech as either the "terrorist surveillance program" or "the NSA's terrorist surveillance program." (U)

IV. Testimony and Other Statements (U)

After the New York Times articles disclosed aspects of the NSA program, members of Congress expressed concern that the President had exceeded his authority by authorizing electronic surveillance activity without FISA orders, and congressional hearings were held on the issue. Gonzales testified before the Senate Judiciary Committee on February 6, 2006, and July 24, 2007, about the NSA's surveillance activities. We describe in the next sections his testimony and other statements he made about the NSA's activities, as well as testimony by former Deputy Attorney General Comey before the Senate Judiciary Committee on May 15, 2007. ~~(TS//SI//NF)~~

---

we found to the "terrorist surveillance program" in connection with the NSA electronic surveillance activities was in NewsMax, an online news website, on December 22, 2005. (U) See "Barbara Boxer: Bush Spy Hearings Before Alito," NewsMax.com, December 22, 2005, http://archive.newsmax.com/archives/ic/2005/12/22/173255.shtml. On January 20, 2006, the term appeared again on another Internet blog called "RedState." See "Making the case for the NSA terrorist surveillance program," at http://www.redstate.com/story/2006/1/20/92730 /0977. (U)

A. Gonzales's February 6, 2006, Senate Judiciary Committee Testimony (U)

In his opening statement before the Senate Judiciary Committee on February 6, 2006, Gonzales began by saying that his testimony would necessarily be limited:

> Before going any further, I should make clear what I can discuss today. I am here to explain the Department's assessment that the President's terrorist surveillance program is consistent with our laws and Constitution. I am not here to discuss the operational details of that program, or any other classified activity. The President has described the terrorist surveillance program in response to certain leaks, and my discussion in this open forum must be limited to those facts the President has publicly confirmed – nothing more. Many operational details of our intelligence activities remain classified and unknown to our enemy – and it is vital that they remain so. (U)

The questioning of Gonzales at this hearing focused primarily on the nature of the NSA surveillance activity and the legal basis for it.[438] Senator Charles Schumer asked Gonzales specifically about accounts of a disagreement within the Justice Department over the NSA program:

> SEN. SCHUMER: But it's not just Republican senators who seriously question the NSA program, but very high-ranking officials within the administration itself. Now, you've already acknowledged that there were lawyers in the administration who expressed reservations about the NSA program. There was dissent. Is that right?
>
> ATTY GEN. GONZALES: Of course, Senator. As I indicated, this program implicates very difficult issues. The war on terror has generated several issues that are very, very complicated.
>
> SEN. SCHUMER: Understood.
>
> ATTY GEN. GONZALES: Lawyers disagree.

---

[438] Neither the Chairman of the Senate Judiciary Committee at the time (Senator Specter), nor the Ranking Member (Senator Leahy), were read into the program or provided the underlying documents authorizing the program. Senator Leahy stated at the outset of the hearing that he and others had made a request to review the Presidential Authorizations and OLC memoranda about the program, but that these materials had not been provided to the Committee. (U)

SEN. SCHUMER: I concede all those points. Let me ask you about some specific reports. It's been reported by multiple news outlets that the former number two man in the Justice Department, the premier terrorism prosecutor, Jim Comey, expressed grave reservations about the NSA program, and at least once refused to give it his blessing. Is that true?

ATTY GEN. GONZALES: Senator, here's a response that I feel that I can give with respect to recent speculation or stories about disagreements. There has not been any serious disagreement, including – and I think this is accurate – there's not been any serious disagreement about the program that the President has confirmed.

There have been disagreements about other matters regarding operations, which I cannot get into. I will also say –

SEN. SCHUMER: But there was some – I'm sorry to cut you off. But there was some dissent within the administration, and Jim Comey did express at some point – that's all I asked you – some reservation.

ATTY GEN. GONZALES: The point I want to make is that, to my knowledge, none of the reservations dealt with the program that we're talking about today. They dealt with operational capabilities that we're not talking about today.

SEN. SCHUMER: I want to ask you again about – I'm just – we have limited time.

ATTY GEN. GONZALES: Yes, sir.

SEN. SCHUMER: It's also been reported that the head of the Office of Legal Counsel, Jack Goldsmith, a respected lawyer and professor at Harvard Law School, expressed reservations about the program. Is that true?

ATTY GEN. GONZALES: Senator, rather than going individual by individual –

SEN. SCHUMER: No, I think we're – this is –

ATTY GEN. GONZALES: – let me just say that I think differing views that have been the subject of some of these stories does not – did not deal with the program that I'm here testifying about today.

SEN. SCHUMER: But you are telling us that none of these people expressed any reservations about the ultimate program. Is that right?

ATTY GEN. GONZALES: Senator, I want to be very careful here, because, of course, I'm here only testifying about what the President has confirmed. And with respect to what the President has confirmed, I believe – I do not believe that these DOJ officials that you're identifying had concerns about this program. (U)

Throughout the hearing, other Senators asked Gonzales questions relating to various aspects of the NSA program, and Gonzales would often qualify his answers by stating that he was not discussing activities beyond what the President had confirmed. However, in doing so Gonzales sometimes suggested that the NSA's activities under the program were limited to what the President had confirmed. In one exchange with Senator Leahy, for example, Gonzales suggested that the electronic surveillance activities the President had publicly confirmed were the only activities the President had authorized to be conducted. Specifically, in response to a series of questions from Senator Leahy regarding what activities beyond warrantless electronic surveillance Gonzales would deem legal under the Authorization for the Use of Military Force, Gonzales stated,

> Sir, I have tried to outline for you and the committee what the President has authorized, and that is all that he has authorized. . . . There is all kinds of wild speculation out there about what the President has authorized and what we're actually doing. And I'm not going to get into a discussion, Senator, about hypotheticals.[439] ~~(S//NF)~~

---

[439] On February 28, 2006, Gonzales wrote to Senator Specter to provide additional responses to questions that he had answered during his February 6 hearing and to clarify certain responses. Gonzales wrote that he confined his letter and testimony

> to the specific NSA activities that have been publicly confirmed by the President. Those activities involve the interception by the NSA of the contents of communications in which one party is outside the United States where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization (hereinafter, the "Terrorist Surveillance Program").

One response Gonzales sought to clarify was this response to Senator Leahy. Gonzales wrote:

> First, as I emphasized in my opening statement, in all of my testimony at the hearing I addressed – with limited exceptions – only the legal underpinnings of the Terrorist Surveillance Program, as defined above. I did not and could not address operational aspects of the Program or any other classified intelligence activities. So, for example, when I testified in response to questions from Senator Leahy, "Sir, I have tried to outline for you and the Committee what the President has authorized, and that is all that he has authorized," Tr. at 53, I was confining my remarks to the Terrorist

(Cont'd.)

In response to Senator Sam Brownback's question about whether the FISA application process would include "even these sort of operations we've read about data mining operations? Would that include those sorts of operations, or are those totally a separate type of field?" (U)

Gonzales responded:

> I'm not here to talk about that. Again, let me just caution everyone that you need to read these stories with caution. There is a lot of mumbling – I mean, mixing and mangling of activities that are totally unrelated to what the President has authorized under the terrorist surveillance program, and so I'm uncomfortable talking about other kinds of operations that might – that are unrelated to the terrorist surveillance program. (U)

B. Comey's May 15, 2007, Senate Judiciary Committee Testimony (U)

Former Deputy Attorney General Comey appeared before the Senate Judiciary Committee on May 15, 2007, in a hearing called to examine whether the Department had politicized the firing of U.S. Attorneys. Senator Schumer, who presided over the hearing, began the questioning by asking Comey about reports in the media that in March 2004 White House Counsel Gonzales and White House Chief of Staff Card had visited Attorney General Ashcroft in the hospital in an effort to override Comey's decision, made when he served as Acting Attorney General, not to certify a classified program. Comey was asked to recount the details of the incident. (U)

After prefacing his remarks by stating that he could not discuss classified information, Comey described the events of March 2004, including the confrontation between the Department and White House officials in Ashcroft's hospital room. In describing these events, Comey referred to a single classified program. For example, Comey testified that:

> In the early part of 2004, the Department of Justice was engaged – the Office of Legal Counsel, under my supervision, in a reevaluation both factually and legally of a particular classified program. And it was a program that was renewed on a regular basis and required signature by the Attorney General

---

Surveillance Program as described by the President, the legality of which was the subject of the February 6th hearing.

Gonzales also attempted to clarify a response he had given to Senator Leahy about when the first Presidential Authorization was signed. Gonzales wrote that "The President first authorized the [Terrorist Surveillance] Program in October 2001 . . . ." (U)

> certifying to its legality. And the – and I remember the precise date; the program had to be renewed by March the 11th, which was a Thursday, of 2004. And we were engaged in a very intensive reevaluation of the matter. (U)

Comey also testified that "as Acting Attorney General, I would not certify the program as to its legality, and explained our reasoning in detail, which I will not go into here, nor am I confirming it's any particular program." As detailed in Chapter Four, Comey then described from his perspective the incident in the hospital room and testified that after that incident "[t]he program was reauthorized without us, without a signature from the Department of Justice attesting as to its legality . . . ." (U)

C. Gonzales's June 5, 2007, Press Conference (U)

In light of Comey's statements, questions were raised about the accuracy of Gonzales's February 2006 testimony to the Senate Judiciary Committee. For example, in a press conference on June 5, 2007, called to announce the indictment of members of an international gang called MS-13, the first question a reporter asked Gonzales concerned Comey's testimony:

> REPORTER: Attorney General, last month Jim Comey testified about visits you and Andy Card made to John Ashcroft's hospital bed. Can you tell us your side of the story? Why were you there and did Mr. Comey testify truthfully about it? Did he remember it correctly?
>
> ATTY GEN. GONZALES: Mr. Comey's testimony related to a highly classified program which the President confirmed to the American people some time ago. Because it's on a classified program I'm not going to comment on his testimony. (U)

As discussed below, when later asked about this statement, Gonzales said that he had misspoke, and that he did not mean to say that Comey's testimony related to the program that the President confirmed. (U)

D. Gonzales's July 24, 2007, Senate Judiciary Committee Testimony (U)

Gonzales was again called to testify before the Senate Judiciary Committee on July 24, 2007. In advance of Gonzales's July 24 appearance, Senator Leahy sent Gonzales a letter advising him of the questions that would be asked at the hearing.[440] The letter referenced Gonzales's

---

[440] According to the letter, Senator Leahy took this step because in Gonzales's appearance before the Senate Judiciary Committee on April 19, 2007, to discuss the removal of nine U.S. Attorneys, Gonzales had responded to an estimated 100 questions that (Cont'd.)

February 6, 2006, testimony in which he stated that Department officials did not have "concerns about this program." The letter also referenced Comey's May 15 testimony concerning the incident in Ashcroft's hospital room in March 2004. The letter specifically advised Gonzales that he would be asked to "provide a full explanation for the legal authorization for the President's warrantless electronic surveillance program in March and April 2004." (U)

At the July 24 hearing, Gonzales was repeatedly questioned about alleged inconsistencies between his and Comey's accounts of the events of March 2004 and the NSA program. For example, Senator Specter asked:

> Let me move quickly through a series of questions – there's a lot to cover – starting with the issue that Mr. Comey raises. You said, quote, "There has not been any serious disagreement about the program." Mr. Comey's testimony was that Mr. Gonzales began to discuss why they were there to seek approval and he then says, quote, "I was very upset. I was angry. I thought I had just witnessed an effort to take advantage of a very sick man."
>
> First of all, Mr. Attorney General, what credibility is left for you when you say there's no disagreement and you're party to going to the hospital to see Attorney General Ashcroft under sedation to try to get him to approve the program?
>
> ATTY GEN. GONZALES: The disagreement that occurred and the reason for the visit to the hospital, Senator, was about other intelligence activities. It was not about the terrorist surveillance program that the President announced to the American people. (U)

At other points in the hearing, Gonzales stated that the dispute referred to "other intelligence activities," and not the "terrorist surveillance program." (U)

Senator Schumer also questioned Gonzales about his answer in the June 5 press conference in which he stated that Comey's testimony "related to a highly classified program which the President confirmed to the American people some time ago." Gonzales first responded that he would have to look at the question and his response from the press conference, and then he said "I'm told that what I'd in fact – here in the press

---

he could "not recall." Leahy wrote that he wanted to assist Gonzales with his preparation for the July 24 testimony to "avoid a repeat of that performance." (U)

conference – I did misspeak, but I also went back and clarified it with the reporter."[441] (U)

Gonzales then responded to Senator Schumer that "The President confirmed the existence of one set of activities," and that "Mr. Comey was talking about a disagreement that existed with respect to other intelligence activities. . . . Mr. Comey's testimony about the hospital visit was about other intelligence activities, disagreements over other intelligence activities. That's how we'd clarify it." (U)

Other Senators questioned Gonzales's responses on this issue. For example, Senator Feingold stated:

> With respect to the NSA's illegal wiretapping program, last year in hearings before this committee and the House Judiciary Committee, you stated that, quote, "There has not been any serious disagreement about the program that the President has confirmed," unquote, that any disagreement that did occur, quote, "did not deal with the program that I am here testifying about today," unquote, and that, quote, "The disagreement that existed does not relate to the program the President confirmed in December to the American people," unquote. (U)
>
> Two months ago, you sent a letter to me and other members of this committee defending that testimony and asserting that it remains accurate. And I believe you said that again today. Now, as you probably know, I'm a member of the Intelligence Committee. And therefore I'm one of the members of this committee who has been briefed on the NSA wiretapping program and other sensitive intelligence programs. I've had the opportunity to review the classified matters at issue here. And I believe that your testimony was misleading, at best. I am prevented from elaborating in this setting, but I intend to send you a classified letter explaining why I have come to that conclusion. (U)

Senator Whitehouse, also a member of the Intelligence Committee, similarly stated:

> Mr. Gonzales, let me just follow up briefly on what Senator Feingold was saying, because I'm also a member of both committees. And I have to tell you, I have the exact same

---

[441] Gonzales also testified that he did not speak directly to the reporter (Dan Eggen, from the Washington Post) to clarify the comment. Rather, Gonzales said he told a Department spokesperson to go back and clarify the statement to Eggen. (U)

perception that he does, and that is that if there is a kernel of truth in what you've said about the program which we can't discuss but we know it to be the program at issue in your hospital visit to the Attorney General, the path to that kernel of truth is so convoluted and is so contrary to the plain import of what you said, that I, really, at this point have no choice but to believe that you intended to deceive us and to lead us or mislead us away from the dispute that the Deputy Attorney General subsequently brought to our attention. So you may act as if he's behaving, you know, in a crazy way to even think this, but at least count two of us and take it seriously.[442] (U)

Gonzales also offered to answer a question about the terrorist surveillance program in closed session during this exchange with Senator Specter:

SEN. SPECTER: Going back to the question about your credibility on whether there was dissent within the administration as to the terrorist surveillance program, was there any distinction between the terrorist surveillance program in existence on March 10th, when you and the Chief of Staff went to see Attorney General Ashcroft, contrasted with the terrorist surveillance program which President Bush made public in December of 2005?

ATTY GEN. GONZALES: Senator, this is a question that I should answer in a classified setting, quite frankly, because now you're asking me to hint or talk – to hint about our operational activities. And I'd be happy to answer that question, but in a classified setting.

SEN. SPECTER: Well, if you won't answer that question, my suggestion to you, Attorney General Gonzales, is that you review this transcript very, very carefully. I do not find your testimony credible, candidly. When I look at the issue of credibility, it is my judgment that when Mr. Comey was testifying he was talking about the terrorist surveillance program and that inference arises in a number of ways, principally because it was such an important matter that led you and the Chief of Staff to Ashcroft's hospital room. . . . So my suggestion to you is that you review your testimony very carefully. The chairman's already said that the committee's

[442] According to a May 17, 2006, letter from the Director of National Intelligence, two other members of the Judiciary Committee – Senators Dianne Feinstein and Orrin Hatch – also had been briefed on the NSA program. (U)

going to review your testimony very carefully to see if your credibility has been breached to the point of being actionable. (U)

Near the end of the hearing Senator Schumer questioned Gonzales regarding the meeting at the White House with the "Gang of Eight" congressional leaders, just before Gonzales and Card went to Ashcroft's hospital room on March 10, 2004:

> SEN. SCHUMER: OK. But you testified to us that you didn't believe there was serious dissent on the program that the President authorized. And now you're saying they knew of the dissent and you didn't?
>
> ATTY GEN. GONZALES: The dissent related to other intelligence activities. The dissent was not about the terrorist surveillance program the President confirmed and . . .
>
> . . .
>
> SEN. SCHUMER: You said, sir – sir, you said that they knew that there was dissent. But when you testified before us, you said there has not been any serious disagreement. And it's about the same program. It's about the same exact program. You said the President authorized only one before. And the discussion – you see, it defies credulity to believe that the discussion with Attorney General Ashcroft or with this group of eight, which we can check on – and I hope we will, Mr. Chairman: that will be yours and Senator Specter's prerogative -- was about nothing other than the TSP. And if it was about the TSP, you're dissembling to this committee. Now was it about the TSP or not, the discussion on the eighth?
>
> ATTY GEN. GONZALES: The disagreement on the 10th was about other intelligence activities.
>
> SEN. SCHUMER: Not about the TSP, yes or no?
>
> ATTY GEN. GONZALES: The disagreement and the reason we had to go to the hospital had to do with other intelligence activities.
>
> SEN. SCHUMER: Not the TSP? Come on. If you say it's about "other," that implies not. Now say it or not.
>
> ATTY GEN. GONZALES: It was not. It was about other intelligence activities.
>
> SEN. SCHUMER: Was it about the TSP? Yes or no, please? That's vital to whether you're telling the truth to this committee.

ATTY GEN. GONZALES: It was about other intelligence activities. (U)

When we interviewed Gonzales, he stated that there was never any intent to hide the NSA program from Congress, and he said that Congress was briefed on multiple occasions about the program.[443] Gonzales also stated that he could not explain to the Senate Judiciary Committee that the "serious" dispute concerned [redacted] Gonzales said that he could not recall where the term "terrorist surveillance program" originated, but that when he used the term it referred only to the content collection activities the President had confirmed publicly, and that the rest of the program remained classified. Gonzales also asserted that this distinction should have been clear to those on the committee who were read into the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

E. FBI Director Mueller's July 26, 2007, House Committee on the Judiciary Testimony (U)

Two days after Gonzales's July 24, 2007, Senate Judiciary Committee testimony, FBI Director Mueller testified before the House Judiciary Committee. At this hearing, Mueller was asked about his conversation with Attorney General Ashcroft at the hospital on the evening of March 10, 2004. As discussed in Chapter Four of this report, Mueller arrived at the hospital just after Gonzales and Card left. Mueller was asked to recount what he learned from Ashcroft concerning Ashcroft's exchange with Gonzales and Card earlier that evening:

REP. JACKSON LEE: Could I just say, did you have an understanding that the discussion was on TSP?

MR. MUELLER: I had an understanding the discussion was on a – a NSA program, yes.

REP JACKSON LEE: I guess we use "TSP," we use warrantless wiretapping, so would I be comfortable in saying that those were the items that were part of the discussion?

---

[443] Gonzales cited in particular the "Gang of Eight" briefing convened on March 10, 2004, to inform congressional leaders of the Department's legal concerns about aspects of the program and the need for a legislative fix. We also reviewed Gonzales's closed-session testimony before the House Permanent Select Committee on Intelligence (HPSCI), which he provided on July 19, 2007, just a few days before his July 24 Senate Judiciary Committee testimony. In his classified HPSCI testimony, Gonzales stated, "This disagreement [with Justice Department officials] primarily centered on [redacted] ~~(TS//STLW//SI//OC/NF)~~

MR. MUELLER: I – the discussion was on a national – an NSA program that has been much discussed, yes. (U)

We asked Mueller about his understanding of the term "terrorist surveillance program." Mueller said that the term "TSP" was not used by the FBI prior to The New York Times article and the President's confirmation of one aspect of the program. Mueller said he understood the term to refer to what the President publicly confirmed as to content intercepts. Mueller said he believed the term "TSP" was part of the "overarching" Stellar Wind program, but that "TSP" is not synonymous with Stellar Wind.[444] ~~(S//NF)~~

F. Gonzales's Follow-up Letter to the Senate Judiciary Committee (U)

In an effort to clarify his July 24, 2007, Senate testimony, on August 1, 2007, Gonzales sent unclassified letters to Judiciary Committee Chairman Leahy and Senator Specter. Gonzales's letter to Leahy stated that he was deeply concerned with suggestions that his testimony was misleading and he was determined to address any such impression. He explained that "shortly after 9/11, the President authorized the NSA to undertake a number of highly classified activities," and that, "although the legal bases for these activities varied, all of them were authorized in one presidential order, which was reauthorized approximately every 45 days." Gonzales wrote that before December 2005 "the term 'Terrorist Surveillance Program' was not used to refer to these activities, collectively or otherwise." Rather, Gonzales wrote that the term was first used in early 2006 "as part of the public debate that followed the unauthorized disclosure [by the New York Times] and the President's acknowledgement of one aspect of the NSA activities[.]" (U)

---

[444] We also interviewed an NSA official, who serves as an original classifying authority for the NSA, about the use of the term "terrorist surveillance program" or "TSP" at the NSA.

~~(TS//STLW//SI//OC/NF)~~

Gonzales also wrote in this letter that in his July 24 testimony he was discussing "only that particular aspect of the NSA activities that the President has publicly acknowledged, and that we have called the Terrorist Surveillance Program[.]" He wrote that he recognized that his use of this term or his shorthand reference to the "'program' publicly 'described by the President'" may have "created confusion." Gonzales maintained that there was "not a serious disagreement between the Department and the White House in March 2004 about whether there was a legal basis for the particular activity later called the Terrorist Surveillance Program." (U)

Gonzales also wrote in his letter, "That is not to say that the legal issues raised by the Terrorist Surveillance Program were insubstantial; it was an extraordinary activity that presented novel and difficult issues and was, as I understand, the subject of intense deliberations within the Department. In the spring of 2004, after a thorough reexamination of all these activities, Mr. Comey and the Office of Legal Counsel ultimately agreed that the President could direct the NSA to intercept international communications without a court order where the interceptions were targeted at al Qaeda or its affiliates. Other aspects of the NSA's activities referenced in the DNI's letter [attached to Gonzales's letter] did precipitate very serious disagreement." (U)

V. OIG Analysis (U)

In this section, we assess whether Gonzales made false, inaccurate, or misleading statements during his testimony before the Senate Judiciary Committee. As discussed below, we concluded that Gonzales's testimony did not constitute a false statement under the criminal statutes. We also concluded that he did not intend his testimony to be inaccurate, false, or misleading. However, we found in at least two important respects his testimony was confusing, inaccurate, and had the effect of misleading those who were not read into the program. (U)

At the outset, we recognize that Gonzales was in a difficult position because he was testifying in an open, unclassified forum about a highly classified program. In this setting, it would be difficult for any witness to clearly explain the nature of the dispute between the White House and the Department while not disclosing additional details about classified activities, particularly because only certain NSA activities had been publicly confirmed by the President. (U)

However, some of this difficulty was attributable to the White House's decision not to brief the Judiciary Committee, which had oversight of the Department of Justice, about the program. As discussed in Chapter Four, the strict controls over the Department's access to the program hindered the

Department's ability to adequately fulfill its legal responsibilities concerning the program through March 2004. Similarly, the White House's decision not to allow at least the Chair and Ranking Members of the House and Senate Judiciary Committees to be briefed into the program created difficulties for Gonzales when he testified before Congress about the disputes regarding the program. This limitation also affected the Committee's ability to understand or adequately assess the program, especially in connection with the March 2004 dispute. We agree with Goldsmith's observation about the harm in the White House's "over-secrecy" for this program, as well as Director Mueller's suggestion, made in March 2004, that briefings on the program should have been given to the House and Senate Judiciary Committees. This did not occur, and it made Gonzales's testimony to the Senate Judiciary Committee unusually difficult. ~~(TS//SI//NF)~~

Yet, even given these difficulties, we believe that Gonzales's testimony was imprecise, confusing, and likely to lead those not read into the program to draw wrong conclusions about the nature of the dispute between White House and Department officials in March 2004. In addition, two Senators who had been read into the program stated that they were confused by Gonzales's testimony. Although we concluded that Gonzales did not intend to mislead Congress, his testimony nonetheless had the effect of creating confusion and inaccurate perceptions about certain issues covered during his hearings. (U)

Gonzales, as a participant in the March 2004 dispute between the White House and the Justice Department and, more importantly, as the nation's chief law enforcement officer, had a duty to balance his obligation not to disclose classified information with the need not to be misleading in his testimony about the events that nearly led to mass resignations of senior officials at the Justice Department and the FBI. Instead, Gonzales's testimony only deepened the confusion among members of Congress and the public about these matters. We were especially troubled by Gonzales's testimony at the July 2007 Senate hearing because it related to an important matter of significant public interest and because he had sufficient time to prepare for this hearing and the questions he knew he would be asked. (U)

At the outset of his testimony on February 6, 2006, Gonzales explained that he was confining his remarks to the program and the facts that the President publicly confirmed in his radio address on December 17, 2005. In those remarks, the President had, in essence, confirmed the

content collection part, or basket 1, of the NSA surveillance program.[445] The President, and Gonzales, used the term "terrorist surveillance program" in connection with the President's confirmation of these NSA activities. However, as discussed below, it was not clear – even to those read into the program – whether the term "terrorist surveillance program" referred only to content collection (basket 1) or the entire program.
~~(TS//STLW//SI//OC/NF)~~

Nevertheless, Gonzales suggested in his testimony that the dispute between the White House and the Department concerned other intelligence activities that were unrelated to the content collection portion of the program that the President had confirmed. This was not accurate. ~~(S//NF)~~

We recognize that the term "terrorist surveillance program" was intended by Gonzales and other Administration officials to describe a limited set of activities within the Stellar Wind program and that the term was created only in response to public disclosures about the program. However, by using phrases such as the "terrorist surveillance program" or "the program that the President has confirmed," and setting that program distinctly apart from "other intelligence activities," Gonzales's testimony created a perception that the two sets of activities were entirely unrelated, which was not accurate. Gonzales's testimony suggested that the dispute that Comey testified about was not related to the program that the President had confirmed, and instead that the dispute concerned unrelated "operations" or "intelligence activities." Thus, while Gonzales may have intended the term "terrorist surveillance program" to cover only content collection (basket 1), it led to confusion and misperceptions when he testified that the dispute [redacted] was unrelated to "the terrorist surveillance program."
~~(TS//STLW//SI//OC/NF)~~

Gonzales reinforced this misperception throughout his testimony. For example, when asked by Senator Leahy what activities Gonzales believed would be supported under the Authorization for Use of Military Force rationale, Gonzales stated, "I have tried to outline for you and the committee what the President has authorized, and that is all that he has authorized." In fact, the President had authorized two other types of collections in the same Authorization. Gonzales himself subsequently realized that his response to Senator Leahy was problematic. In a February 28, 2006, letter to Senators Specter and Leahy, Gonzales sought to clarify his response,

[redacted]

stating, "I was confining my remarks to the Terrorist Surveillance Program as described by the President, the legality of which was the subject of the February 6th hearing." However, in our view this attempt to clarify his remarks did not go nearly far enough. As discussed below, it was not until after Gonzales's next appearance before the Senate Judiciary Committee in July 2007 that Gonzales acknowledged that the President had also authorized a range of intelligence-gathering activities, including those described under the terrorist surveillance program, in a single order. ~~(TS//STLW//SI//OC/NF)~~

We concluded that Gonzales created a misimpression for Congress and the public by suggesting that the March 2004 dispute between the Department and the White House concerned issues wholly unrelated to "the program the President confirmed," or the terrorist surveillance program. We believe a fairer and more accurate characterization would have been that the March 2004 dispute concerned aspects of a larger program of which the terrorist surveillance program was a part. As discussed earlier, the NSA viewed the three types of collections as a single program. The three types of collections were all authorized by the same Presidential order and administered by a single intelligence agency. Moreover, all three collections were known in the Intelligence Community by the same Top Secret/Sensitive Compartmented Information program cover term, Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

In addition, we believe that Gonzales's testimony regarding the dispute between the Department and the White House [redacted] was incomplete and not accurate. ~~(TS//SI//OC/NF)~~

When Senator Schumer asked Gonzales at the February 2006 Senate hearing whether media accounts that Comey "expressed grave reservations about the NSA program" were true, Gonzales responded that there was no "serious disagreement about the program that the President has confirmed." But there was a dispute about [redacted] As recounted in detail in Chapter Four of this report, [redacted] The dispute involving [redacted] was not resolved, and the March 11, 2004,

Presidential Authorization continued to permit the activity [redacted] ~~(TS//STLW//SI//OC/NF)~~

When we interviewed Gonzales, he told us that he was trying to be careful during his public testimony about discussing or characterizing a classified program with persons not read into the program, and that he used the term "serious disagreement" to distinguish the disagreement regarding [redacted] from other disagreements regarding the program. Gonzales told us that he believed his statement that there was "no serious disagreement" was accurate because he did not consider the Department's conclusion that [redacted] to be a point of "serious disagreement" between the Justice Department and the White House, particularly when compared to the more serious disagreement related to [redacted].[446] Gonzales also told the OIG that he would not have gone to Ashcroft's hospital room solely over [redacted] and other evidence discussed in Chapter Four tends to confirm that [redacted] was not the critical issue in the confrontation with Department officials at the hospital or that it precipitated the threat of mass resignations by senior Department and FBI officials. ~~(TS//STLW//SI//OC/NF)~~

Yet, even if one agrees that [redacted] was not a "serious disagreement" between the Department and the White House, Gonzales's testimony is still problematic. When Senator Schumer pressed Gonzales on whether Department officials "expressed any reservations about the ultimate program," Gonzales replied: "Senator, I want to be very careful here, because, of course, I'm here only testifying about what the President has confirmed. And with respect to what the President has confirmed, I believe – I do not believe that these DOJ officials that you're identifying had concerns about this program." ~~(TS//STLW//SI//OC/NF)~~

We understand that it is possible to construct an argument that the Department officials did not have "reservations" or "concerns" about the [redacted] However, while such an argument at best might be considered technically accurate, it would still not account for key details that were omitted from

[446] While Gonzales may subjectively have believed the disagreement about this issue did not rise to the level of a serious dispute, he was aware that Goldsmith and Addington sharply disagreed about [redacted] ~~(TS//SI//NF)~~

Gonzales's testimony that would be necessary for an accurate understanding of the situation. The Department clearly had reservations and concerns about the [redacted] of the program, [redacted] Moreover, Gonzales himself contradicted this attempted construction by stating in a February 28, 2006, letter to Senator Specter that the terrorist surveillance program was first authorized by the President in October 2001, years before the [redacted] Gonzales knew that Comey, Goldsmith, and others at the Department had expressed "reservations" or "concerns" about [redacted] prior to the President's decision to [redacted] ~~(TS//STLW//SI//OC/NF)~~

While we believe the evidence does show that [redacted] was more significant than the dispute about [redacted] the evidence is clear that Comey and others had strong and clearly identified concerns regarding the extent of the President's authority to conduct [redacted] These concerns had been communicated to the White House in several meetings over a period of months prior to and including March 2004, and the White House did not [redacted] part of the program in response to these concerns. However, Gonzales's testimony suggested that such concerns and reservations on the part of Justice Department officials never existed. To the contrary, the Department's firm objections to this aspect of the program were instrumental in bringing about [redacted] collection in "the program the President has confirmed." ~~(TS//STLW//SI//OC/NF)~~

Following his July 24, 2007, testimony, Gonzales acknowledged in an unclassified August 1, 2007, letter to Senator Leahy that his use of the term "terrorist surveillance program" and his "shorthand reference to the 'program' publicly 'described by the President' may have created confusion," particularly for those familiar with the full range of NSA activities authorized by the President. Gonzales wrote that he was determined to address any impression that his testimony was misleading. In this letter, Gonzales attempted to describe what he had meant by the term "terrorist surveillance program," stating that it covered one aspect of the NSA activities that the President had authorized. His letter also acknowledged the dispute concerned the legal basis for certain NSA activities that were regularly authorized in the same Presidential Authorization as the terrorist surveillance program. Gonzales also acknowledged that Comey had refused to certify a Presidential Authorization "because of concerns about the legal basis of certain of these NSA activities." Yet, this follow-up letter, while providing more context about the issues than his July 2007 statements, did not completely address the misimpressions created by his testimony.

Gonzales still suggested in his August 1 letter that the only dispute between the Department and the White House concerned aspects of the program [redacted] ~~(TS//STLW//SI//OC/NF)~~

While we again acknowledge the difficulty of the situation Gonzales faced in testifying publicly about a highly classified and controversial program, we believe Gonzales could have done other things to provide clearer and more accurate testimony without divulging classified information. Similar to the import of his August 1 letter, and without providing operational details about these other activities, he could have clarified that part of the dispute with the Department concerned the scope of what he called "the terrorist surveillance program," while another part of the dispute concerned other "intelligence activities" that were either related to the terrorist surveillance program or, more accurately, a different aspect of the same NSA program. Gonzales also could have explained that different activities under the program raised different concerns within the Department because each set of activities rested upon different legal theories.[447] ~~(S//NF)~~

Alternatively, Gonzales could have declined to discuss any aspect of the dispute at an open hearing.[448] Or, short of seeking a closed session, Gonzales could have sought White House approval to brief the Chairs and Ranking Members of the Senate and House Judiciary Committees about the program so that they would fully understand the nature of the NSA program and the classified issues surrounding the dispute. Instead, Gonzales gave public testimony that was confusing and inaccurate, and had the effect of misleading those who were not read into the program, as well as some who were. (U)

Concerning Gonzales's July 2007 testimony in particular, the questions Gonzales would be expected to answer were clearly foreseeable, especially in light of the disparities between his February 6, 2006, testimony and Comey's May 15, 2007, testimony. In addition, Gonzales had been provided a letter by Senator Leahy referencing Comey's testimony and advising Gonzales to be prepared to discuss the legal authorization for the "President's warrantless electronic surveillance program in March and April

[447] [redacted]

[448] As noted, Gonzales provided closed-session testimony before HPSCI on July 19, 2007, in which he described the March 2004 dispute between White House and Justice Department officials as [redacted] ~~(TS//STLW//SI//OC/NF)~~

2004." Gonzales was therefore on notice that he would be expected to bring clarity to the confusion that existed following Comey's testimony. Rather than clarify these matters, we believe Gonzales further confused the issues through his testimony. (U)

Finally, we considered whether Gonzales's testimony constituted criminal false statements and concluded that his statements did not constitute a criminal violation of 18 U.S.C. § 1001. A person violates that statute by "knowingly and willfully" making a "materially false, fictitious, or fraudulent statement or representation[.]" 18 U.S.C. § 1001(a)(2). We do not believe the evidence showed that Gonzales intended to mislead Congress or willfully make a false statement. Moreover, we do not believe a prosecutor could prove beyond a reasonable doubt that there was no interpretation of his words that could be viewed as literally true, even if his testimony was confusing and created misperceptions.[449] (U)

In sum, we believe that while the evidence did not show that Gonzales's statements constitute a criminal violation, or that he intended to mislead Congress, his testimony was confusing, not accurate, and had the effect of misleading those who were not knowledgeable about the program. His testimony also undermined his credibility on this important issue. As the Attorney General, we believe Gonzales should have taken more care to ensure that his testimony was as accurate as possible without revealing classified information, particularly given the significance of this matter and the fact that aspects of the dispute had been made public previously. (U)

---

[449] See *United States v. Milton*, 8 F.3d 39, 45 (D.C. Cir. 1993)("defense of literal truth" applies to false statement prosecutions under 18 U.S.C. § 1001), *cert. denied*, 513 U.S. 919 (1994). See also *United States v. Hsia*, 24 F. Supp. 2d 33 (D.D.C. 1998), in which the court stated, "A false statement is an essential element of a prosecution under 18 U.S.C. § 1001, and if the statement at issue is literally true a defendant cannot be convicted of violating Section 1001." Id. at 58; *United States v. Hsia*, 176 F.3d 517, 525 (D.C. Cir. 1999)(reversing on other grounds). (U)

CHAPTER NINE
CONCLUSIONS (U)

Within weeks of the terrorist attacks of September 11, 2001, the National Security Agency (NSA) initiated a Top Secret, compartmented program to collect and analyze international and domestic telephone and e-mail communications and related data. The intent of the NSA program, which used the cover term Stellar Wind, was to function as an "early warning system" to detect and prevent future terrorist attacks within the United States. ~~(TS//STLW//SI//OC/NF)~~

The program was authorized by the President in a series of Presidential Authorizations that were issued at approximately 30 to 45 day intervals and certified as to form and legality by the Attorney General. The Presidential Authorizations stated that an extraordinary emergency existed permitting the use of electronic surveillance within the United States for counterterrorism purposes, without a court order, under specified circumstances. Under the program the NSA collected vast amounts of information through electronic surveillance and other intelligence-gathering techniques, including information concerning the telephone and e-mail communications of American citizens and other U.S. persons. Top Secret compartmented information derived from this collection was provided to, among other agencies, the FBI, which sent Secret-level, non-compartmented versions of the information to FBI field offices as investigative leads. ~~(TS//STLW//SI//OC/NF)~~

The Stellar Wind program represented an extraordinary expansion of the NSA's signals intelligence activity and a departure from the traditional restrictions on electronic surveillance imposed under the Foreign Intelligence Surveillance Act (FISA), Executive Order 12333, and other laws. Yet, the program was conducted with limited notification to Congress and without judicial oversight, even as the program continued for years after the September 11 attacks. ~~(TS//STLW//SI//OC/NF)~~

The White House tightly controlled who within the Justice Department could be read into the Stellar Wind program. In particular, we found that only three Department attorneys, including the Attorney General, were read into the program and only one attorney was assigned to assess the program's legality in its first year and a half of operation. The limited number of Justice Department read-ins contrasted sharply with the hundreds of operational personnel who were read into the program at the FBI and other agencies involved with the program. ~~(TS//STLW//SI//OC/NF)~~

I. Operation of the Program (U//~~FOUO~~)

Under the program, the NSA initially intercepted the content of international telephone and e-mail communications in cases where at least one of the communicants was reasonably believed to be associated with any international terrorist group. These collections became known as basket 1 of the Stellar Wind program. [redacted] (~~TS//STLW//SI//OC/NF~~)

The NSA also collected bulk telephony and e-mail meta data – communications signaling information showing contacts between and among telephone numbers and e-mail addresses, but not the contents of those communications. These collections became known as basket 2 (telephone meta data) and basket 3 (e-mail meta data) of the Stellar Wind program. (~~TS//STLW//SI//OC/NF~~)

Under basket 2 collections, [redacted] These call detail records included the originating and terminating telephone number of each call, and the date, time, and duration of each call, but not the content of the call. The NSA collected [redacted] "pairs" of contacts per day, including all domestic and international telephone calls [redacted] (~~TS//STLW//SI//OC/NF~~)

Regarding e-mail meta data (basket 3), the NSA collected and archived [redacted] Internet traffic [redacted][450] E-mail meta data included only the "to," "from," "cc," "bcc," and other addressing-type information, but similar to call detail records did not include the subject line or the message contents. (~~TS//STLW//SI//OC/NF~~)

NSA analysts accessed baskets 2 and 3 for analytical purposes with specific telephone numbers or e-mail addresses that satisfied the standard

[450] [redacted]

for querying the data as described in the Presidential Authorizations. A small amount of the collected content and meta data was analyzed by the NSA, working with other members of the Intelligence Community, to generate intelligence reports about suspected terrorists and individuals possibly associated with them. Many of these reports were disseminated, or "tipped," to the FBI for further dissemination as leads to FBI field offices. As of March 2006, [redacted] individual U.S. telephone numbers [redacted] e-mail addresses had been tipped to the FBI, the vast majority of which were disseminated to FBI field offices for investigation or other action. The results of these investigations were uploaded into FBI databases. b1, b3, b7E ~~(TS//STLW//SI//OC/NF)~~

The Justice Department had two primary roles in the Stellar Wind program. First, the Attorney General was required to certify each Presidential Authorization as to form and legality – in effect, to give the Department's assurance that the activities the President was authorizing the NSA to conduct were legal. In carrying out this responsibility, the Attorney General was advised by the Department's Office of Legal Counsel (OLC). As we described in this report and discuss in the next section, we found that during the early phase of the Stellar Wind program the Department lacked sufficient attorney resources to be applied to the legal review of the program and, due in significant part to the White House's extremely close hold over the program, was not able to coordinate its legal review of the program with the NSA. ~~(TS//STLW//SI//OC/NF)~~

The Department's other primary role in Stellar Wind was as a member of the Intelligence Community. The FBI was one of two main customers of the intelligence produced under the program (the other being the CIA). Working with the NSA, a small team of FBI personnel converted the NSA's Top Secret Stellar Wind intelligence reports into leads that were disseminated at the Secret level, under an FBI program called [redacted] to FBI field offices for appropriate action. As detailed in Chapter Six and discussed below, we concluded that although the information produced under the Stellar Wind program had value in some counterterrorism investigations, it played a limited role in the FBI's overall counterterrorism efforts. b1, b3, b7E ~~(TS//STLW//SI//OC/NF)~~

II. Office of Legal Counsel's Analysis of the Stellar Wind Program ~~(TS//SI//NF)~~

As described in Chapters Three, Four, and Five of this report, the Justice Department advised the Executive Branch, and in particular the President, as to the legality of the Stellar Wind program. The Department's view of the legal support for the activities conducted under the program changed over time as more attorneys were read into the program. These

changes occurred in three phases. In the first phase of the program (September 2001 through May 2003), the legality of the program was founded on an analysis developed by John Yoo, a Deputy Assistant Attorney General in OLC. In the second phase (May 2003 through May 2004), the program's legal rationale underwent significant review and revision by OLC Assistant Attorney General Jack Goldsmith and Associate Deputy Attorney General Patrick Philbin. In the third and final phase (July 2004 through January 2007), based in part upon the legal concerns raised by the Department, the entire program was moved from presidential authority to statutory authority under FISA, with oversight by the FISA Court. ~~(TS//STLW//SI//OC/NF)~~

In Chapters Three and Four, we examined the Department's early role in assessing the legality of the Stellar Wind program. The Justice Department's access to the program was controlled by the White House, and former White House Counsel and Attorney General Alberto Gonzales told the OIG that the President decided whether non-operational personnel, including Department lawyers, could be read into the program. Department and FBI officials told us that obtaining approval to read in Department officials and FISA Court judges involved justifying the requests to Counsel to the Vice President David Addington and White House Counsel Gonzales, who effectively acted as gatekeepers to the read-in process for non-operational officials. In contrast, according to the NSA, operational personnel at the NSA, CIA, and the FBI were read into the program on the authority of the NSA Director, who at some point delegated this authority to the Stellar Wind Program Manager. ~~(TS//SI//NF)~~

We believe the White House's policy of limiting access to the program for non-operational personnel was applied at the Department of Justice in an unnecessarily restrictive manner prior to March 2004, and was detrimental to the Department's role in the operation of the program from its inception through that period. We also believe that Attorney General Ashcroft, as head of the Department during this time, was responsible for seeking to ensure that the Department had adequate attorney resources to conduct a thorough and accurate review of the legality of the program. We believe that the circumstances as they existed as early as 2001 and 2002 called for additional Department resources to be applied to the legal review of the program. As noted in Chapter Three, Ashcroft requested to have his Chief of Staff and Deputy Attorney General Larry Thompson read into the program, but the White House did not approve this request. However, because Ashcroft did not agree to be interviewed by the OIG for this investigation, we were unable to determine the full extent of his efforts to press the White House to read in additional Department officials between the program's inception in October 2001 and the critical events of March 2004. ~~(TS//SI//NF)~~

Although we could not determine exactly why Yoo remained the only Department attorney assigned to assess the program's legality from 2001 until his departure in May 2003, we believe that this practice represented an extraordinary and inappropriate departure from OLC's traditional review and oversight procedures and resulted in significant harm to the Department's role in the program. ~~(TS//SI//NF)~~

In the earliest phase of the program, Yoo advised Attorney General Ashcroft and the White House that the collection activities under Stellar Wind were a lawful exercise of the President's inherent authorities as Commander-in-Chief under Article II of the Constitution, subject only to the Fourth Amendment's reasonableness standard. In reaching this conclusion, Yoo dismissed as constitutionally incompatible with the President's Article II authority the FISA statute's provision that FISA was to be the "exclusive means" for conducting electronic surveillance in the United States for foreign intelligence purposes, and he concluded that these statutory provisions should be read to avoid conflicts with the President's constitutional Commander-in-Chief authority. ~~(TS//STLW//SI//OC/NF)~~

As noted above, during the first year and a half of the Stellar Wind program only three Department attorneys were read into the program – Yoo, Attorney General Ashcroft, and James Baker, Counsel in the Office of Intelligence Policy and Review. Jay Bybee, the OLC Assistant Attorney General and Yoo's direct supervisor, was not read into the program and was unaware that Yoo was providing advice on the legal basis to support the program. Thus, Yoo was providing legal opinions on this unprecedented expansion of the NSA's surveillance authority without review by his OLC supervisor or any other Department attorney. Rather, Yoo worked alone on this project, and produced two major opinions supporting the legality of the program. ~~(TS//STLW//SI//OC/NF)~~

When additional attorneys were read into the program in 2003, they provided a fresh review of Yoo's legal memoranda. Patrick Philbin, an Associate Deputy Attorney General, and later Jack Goldsmith, Bybee's replacement as the Assistant Attorney General for OLC, concluded that Yoo's analysis was seriously flawed, both factually and legally. Goldsmith and Philbin concluded that Yoo's analysis fundamentally mischaracterized [redacted] by failing to address the fact that the NSA was collecting [redacted] and also failing to assess the legality of this activity as it was carried out by the NSA. Goldsmith and Philbin also pointed to Yoo's assertion that Congress had not sought to restrict presidential authority to conduct warrantless searches in the national security area, and criticized Yoo's omission from his analysis of a FISA provision (50 U.S.C. § 1811) that addressed the President's authority to conduct electronic surveillance during wartime. They further noted that Yoo based his assessment of the program's legality on an extremely

aggressive view of the law that revolved around the Constitutional primacy of the President's Article II Commander-in-Chief powers, and he may have done so based on a faulty understanding of key elements of the program. ~~(TS//STLW//SI//OC/NF)~~

As described in Chapter Four, Goldsmith and Philbin's reassessment of the legality of Stellar Wind began after Yoo left the Department in May 2003, and culminated in a 108-page legal memorandum issued on May 6, 2004. That memorandum superseded Yoo's earlier Stellar Wind opinions and premised the legality of the program's electronic surveillance activities on statutory rather than Article II constitutional grounds.[451] As a consequence of this new legal rationale, Department officials concluded that the President's authority to conduct electronic surveillance of the enemy in wartime was [redacted] The Department's advice to the White House that the scope of collection under the program [redacted] was legally problematic led to a contentious dispute in March 2004 (discussed below in Section III). ~~(TS//STLW//SI//OC/NF)~~

We agree with many of the criticisms offered by Department officials regarding the practice of allowing a single Department attorney to develop the legal justification for such a complex and contentious program without critical review both within the Department and by the NSA. These officials told us that errors in Yoo's legal memoranda may have been identified and corrected if the NSA had been allowed to review his work. They also stressed the importance of adhering to OLC's traditional practice of peer review of all OLC memoranda and the need for the OLC Assistant Attorney General, as a Senate-confirmed official, to review and approve all such opinions. ~~(TS//SI//NF)~~

These officials also stated that such review and oversight measures are especially important with regard to legal opinions on classified matters that are not subjected to outside scrutiny. We agree with these officials' comments and note that because programs like Stellar Wind are not subject to the usual external checks and balances on Executive authority, OLC's advisory role is particularly critical to the Executive's understanding of potential statutory and Constitutional constraints on its actions. ~~(TS//SI//NF)~~

[redacted]

~~(TS//STLW//SI//OC/NF)~~

We did not agree with Gonzales's view that it was necessary for national security reasons to limit the number of Department read-ins to those "who were absolutely essential," as distinguished from the numerous operational read-ins who were necessary to the technical implementation of the program. First, the program was as legally challenging as it was technically complex. Just as a sufficient number of operational personnel were read into the program to assure its proper technical implementation, we believe that as many attorneys as necessary should have been read in to assure the soundness of the program's legal foundation. This was not done during at least the first 20 months of the program. ~~(TS//SI//NF)~~

Second, we do not believe that reading in a few additional Department attorneys during the initial phase of the program would have jeopardized national security, especially given the [redacted] operational personnel who were cleared into the program during the same period.[452] In fact, the highly classified nature of the program, rather than constituting an argument for limiting the OLC read-ins to a single attorney, made the need for careful analysis and review within the Department and by the NSA more compelling. ~~(TS//SI//NF)~~

We also found that the expansion of legal thinking and breadth of expertise from reading in additional Department attorneys over time eventually produced more factually accurate and legally comprehensive analyses concerning the program. Increased attorney read-ins also was an important factor in grounding the program on firmer legal footing under FISA. The transition of the program from presidential authority to statutory authority under FISA with judicial oversight was made possible through the collective work of the attorneys who finally were read into the program beginning in 2004. The applications to the FISA Court to effectuate this transition were produced by Department attorneys, working with both legal and technical personnel at the NSA, further reinforcing our view that such coordinated efforts are more likely to produce well-considered legal strategies and analysis. ~~(TS//SI//NF)~~

In addition, as discussed in Chapters Six and Seven, the increase in the number of attorneys read into the program beginning in 2004 helped the Department to more efficiently "scrub" Stellar Wind-derived information in FISA applications and improve the handling of Stellar Wind-related discovery issues in international terrorism prosecutions.
~~(TS//STLW//SI//OC/NF)~~

---

[452] By the end of 2003, only Yoo, Ashcroft, Baker, Philbin, and Goldsmith had been read into Stellar Wind at the Department. [redacted] ~~(TS//SI//NF)~~

III. Hospital Visit and White House Recertification of the Program (U)

In Chapter Four, we describe how the Department's reassessment of Yoo's legal analysis led Deputy Attorney General James Comey, who was exercising the powers of the Attorney General while Ashcroft was hospitalized in March 2004, to conclude that he could not certify the legality of the Stellar Wind program. In response, the President sent Gonzales and Chief of Staff Andrew Card to visit Ashcroft in the hospital to seek his certification of the program, an action Ashcroft refused to take. We believe that the way the White House handled its dispute with the Department about the program – particularly in dispatching Gonzales and Card to Ashcroft's hospital room in an attempt to override Comey's decision – was troubling. ~~(TS//SI//NF)~~

As detailed in Chapter Four, by March 2004 when the Presidential Authorization in effect at that time was set to expire, Goldsmith had already notified the White House several months earlier about the Department's doubts concerning the legality of aspects of the Stellar Wind program. He had made clear that the Department questioned the legality of [redacted] ~~(TS//STLW//SI//OC/NF)~~

When Attorney General Ashcroft was hospitalized and unable to fulfill his duties, Deputy Attorney General Comey assumed the Attorney General's responsibilities. Before the Presidential Authorization was set to expire on March 11, 2004, Comey made clear to senior White House officials, including Vice President Cheney and White House Counsel Gonzales, that the Justice Department could not certify the program as legal. The White House disagreed with the Justice Department's position, and on March 10, 2004, convened a meeting of eight congressional leaders to brief them on the Justice Department's decision not to recertify the program and on the need to continue the program. The White House did not ask Comey or anyone from the Department to participate in this briefing, nor did it notify any Department officials that the briefing had been convened. ~~(TS//SI//NF)~~

Following this congressional briefing, at the direction of President Bush, Gonzales and White House Chief of Staff Andrew Card went to the hospital to seek Attorney General Ashcroft's certification of the Authorization. Again, the White House did not notify any Department officials, including Comey, the ranking Department official at the time, that it planned to take this action. Gonzales's and Card's attempt to persuade Attorney General Ashcroft, who was in the intensive care unit recovering from surgery and according to witnesses appeared heavily medicated, to certify the program over Comey's opposition was unsuccessful. Ashcroft

told Gonzales and Card from his hospital bed that he supported the Department's revised legal position, but that in any event he was not the Attorney General at the time – Comey was.[453] ~~(TS//SI//NF)~~

On March 11, the following day, Gonzales certified the Presidential Authorization as to form and legality. ~~(TS//SI//NF)~~

We agree with Director Mueller's observation that the White House's failure to have Justice Department representation at the congressional briefing and the attempt to persuade Ashcroft to recertify the Authorization without going through Comey "gave the strong perception that the [White House] was trying to do an end run around the Acting [Attorney General] whom they knew to have serious concerns as to the legality of portions of the program." ~~(TS//SI//NF)~~

After Mueller, Comey, and other senior Department and FBI officials made known their intent to resign, the President directed that the issue be resolved, and the program was modified to address the Department's legal concerns. Because we were unable to interview key White House officials, we could not determine for certain what caused the White House to change its position and modify the program, although we believe the prospect of mass resignations at the Department and the FBI was a significant factor in this decision. ~~(TS//SI//NF)~~

We reached several conclusions based on our review of the Department's role in the legal analysis of this program and the events surrounding the dispute between the Department and the White House. First, legal opinions supporting complex national security programs – especially classified programs that press the bounds of established law – should be collaborative products supported by sufficient legal and technical expertise and resources at the Department, working in concert with other participating agencies, with the goal of providing the Executive Branch the most informed and accurate legal advice. By limiting access to this program as it did, the White House undermined the Department's ability to perform its critical legal function. ~~(TS//SI//NF)~~

---

[453] Gonzales stated that even if he knew that Ashcroft was aware Comey opposed recertifying the program, Gonzales would still have wanted to speak with Ashcroft because he believed Ashcroft still retained the authority to certify the program. Gonzales testified before the Senate Judiciary Committee in July 2007 that although there was concern over Ashcroft's condition, "We would not have sought nor did we intend to get any approval from General Ashcroft if in fact he wasn't fully competent to make that decision." Gonzales also testified, "There's no governing legal principle that says that Mr. Ashcroft [. . .] If he decided he felt better, could decide, 'I'm feeling better and I can make this decision, and I'm going to make this decision.'" (U)

Second, we believe that if the OLC's traditional peer review and supervisory procedures had been adhered to at the outset, the prospect that aspects of the program would have rested on a questionable legal foundation for over 2 years would have been greatly mitigated. ~~(TS//SI//NF)~~

Third, we believe that the Department and FBI officials who resisted the pressure to recertify the Stellar Wind program because of their belief that aspects of the program were not legally supportable acted courageously and at significant professional risk. We believe that this action by Department and FBI officials – particularly Ashcroft, Comey, Mueller, Goldsmith, Philbin, and Counsel for Intelligence Policy James Baker – was in accord with the highest professional standards of the Justice Department. ~~(TS//SI//NF)~~

We recommend that when the Department of Justice is involved with such programs in the future, the Attorney General should carefully assess whether the Department has been given adequate resources to carry out its vital function as legal advisor to the President and should aggressively seek additional resources if they are found to be insufficient. We also believe that the White House should allow the Department a sufficient number of read-ins when requested, consistent with national security considerations, to ensure that such sensitive programs receive a full and careful legal review. (U)

IV. Transition of Program to FISA Authority ~~(TS//STLW//SI//OC/NF)~~

We also examined the transition of the Stellar Wind program's collection activities from presidential authority to FISA authority. We believe there were strong considerations that favored attempting to transition the program to FISA sooner than actually happened, especially as the program became less a temporary response to the September 11 attacks and more a permanent surveillance tool. ~~(TS//STLW//SI//OC/NF)~~

Chief among these considerations was the Stellar Wind program's substantial effect on privacy interests of U.S. persons. Under Stellar Wind, the government engaged in an unprecedented collection of information concerning U.S. persons. The President authorized the NSA to intercept, without judicial approval or oversight, the content of international communications involving many U.S. persons and the NSA collected massive amounts of non-content data about U.S. persons' domestic and international telephone calls and e-mail communications. We believe that such broad surveillance and collection activities, particularly for a significant period of time, should be conducted pursuant to statute and

judicial oversight. We also believe that placing these activities under Court supervision provides an important measure of accountability for the government's conduct that is less assured where the activities are both authorized and supervised by the Executive Branch alone.
~~(TS//STLW//SI//OC/NF)~~

The instability of the legal reasoning on which the program rested for several years and the substantial restrictions placed on FBI agents' access to and use of program-derived information due to Stellar Wind's highly classified status were additional reasons for transitioning Stellar Wind's collection activities to FISA authority. We acknowledge that the transition would always have been an enormously complex and time-consuming effort that rested upon novel interpretations and uses of FISA that not all FISA Court judges would authorize. Nevertheless, the events described in this report demonstrate that a full transition to FISA authority was achievable and, in our judgment, should have been pursued earlier.
~~(TS//STLW//SI//OC/NF)~~

V. Impact of Stellar Wind Information on FBI Counterterrorism Efforts (~~S//NF~~)

As a user of Stellar Wind program information, the FBI disseminated leads or "tippers" to FBI field offices. These tippers primarily consisted of specific domestic telephone numbers and e-mail addresses that NSA analysts had determined through meta data analysis were connected to individuals involved with al Qaeda or affiliated groups. The tippers also included content of communications intercepted by the NSA based upon its determination that there was probable cause to believe that a party to the communication was al Qaeda or an affiliated group. From October 2001 through February 2006, the NSA provided the FB[redacted] Stellar Wind tippers, the vast majority of which were domestic telephone numbers. b1, b3, b7E
~~(TS//STLW//SI//OC/NF)~~

The FBI's chief objective during the earliest months of Stellar Wind's operation was to expeditiously disseminate program information to FBI field offices for investigation, while protecting the NSA as the source of the information and the methods used to collect the information. The FBI assigned this task to a small group of personnel from the Telephone Analysis Unit (TAU) at FBI Headquarters. This group developed a straightforward process to receive the Top Secret, compartmented Stellar Wind reports from the NSA, reproduce the information in a non-compartmented, Secret-level format, and disseminate the information in Electronic Communications, or ECs, to the appropriate field offices for investigation. These[redacted] ECs placed restrictions on how the information could be used, instructing field offices that the information b1, b3, b7E

was "for lead purposes only" and could not be used for any legal or judicial purpose. ~~(TS//STLW//SI//OC/NF)~~

The FBI's participation in Stellar Wind evolved over time as the program became less a temporary response to the September 11 attacks and more a permanent surveillance capability. As Stellar Wind continued to be reauthorized, the FBI tried to improve the effectiveness of its participation in the program. Most significantly, in February 2003 a team of FBI personnel (Team 10) was assigned to work full-time at the NSA to manage the FBI's participation in the program. ~~(TS//SI//NF)~~

Team 10's chief responsibility was to disseminate Stellar Wind information to FBI field offices. However, over time Team 10 began to participate in Stellar Wind in other ways. For example, Team 10 submitted telephone numbers and e-mail addresses to the NSA for possible querying against the bulk meta data collected under the program, and Team 10 regularly contributed to the NSA's drafting process for Stellar Wind reports. Overall, we found that the decision to assign Team 10 to the NSA improved the FBI's knowledge about Stellar Wind operations and gave the NSA better insight about how FBI field offices investigated Stellar Wind information. These benefits translated to improvements in the Stellar Wind report drafting process, and by extension, in [redacted] leads. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

One of the other changes the FBI implemented to attempt to improve the process for handling Stellar Wind leads was to make the FBI's Headquarters-based Communications Analysis Unit (CAU), instead of the field offices, responsible for issuing National Security Letters (NSL) to obtain subscriber information on tipped telephone numbers and e-mail addresses. This measure, initiated in July 2003, was intended to address agent concerns that the leads, which reproduced the information in a non-compartmented, Secret-level format, did not provide sufficient information to initiate national security investigations, a prerequisite under Justice Department investigative guidelines to issuing NSLs. Agents complained that the ECs suffered from vagueness about the source of the information being provided and lacked factual details about the individuals allegedly involved with al Qaeda and with whom the domestic numbers being disseminated possibly were in contact. ~~(TS//STLW//SI//OC/NF)~~

We found that the CAU implemented this change by issuing NSLs from the [redacted] control file, the non-investigative file created in September 2002 as a repository for [redacted]-related communications between FBI Headquarters and field offices. Issuing NSLs from a control file instead of an investigative file was contrary to internal FBI policy. In November 2006, the FBI finally opened an investigative file for the [redacted] project. We believe the CAU and OGC officials involved in the decision b1, b3, b7E

to issue NSLs from the [redacted] control file concluded in good faith that the FBI had sufficient predication either to connect the [redacted] NSLs with existing preliminary or full investigations of al Qaeda and affiliated groups or to open new preliminary or full investigations in compliance with Justice Department investigative guidelines. However, we concluded that the FBI could have, and should have, opened an investigative file for [redacted] when the decision was first made to have FBI Headquarters instead of field offices issue NSLs for [redacted] leads. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

We also tried to assess the general role of Stellar Wind information in FBI investigations and its value to the FBI's overall counterterrorism efforts. Similar to the FBI, we had difficulty assessing the specific value of the program to the FBI's counterterrorism activities. ~~(S//NF)~~

The majority of Stellar Wind information the NSA provided the FBI related to domestic telephone numbers and e-mail addresses the NSA had identified through meta data analysis as having connections to al Qaeda or affiliated organizations. [redacted] Not surprisingly, FBI agents and analysts with experience investigating [redacted] leads told us that most leads were determined not to have any connection to terrorism. These agents and analysts did not identify for us any specific cases where [redacted] leads helped the FBI identify previously unknown subjects involved in terrorism, although we recognize that FBI officials and agents other than those we interviewed may have had different experiences with Stellar Wind information. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

Two FBI statistical studies that attempted to assess the value of Stellar Wind meta data leads to FBI counterterrorism efforts did not reach explicit conclusions on the program's usefulness. The first study found that 1.2 percent of Stellar Wind leads made "significant" contributions.[454] The second study did not identify any examples of "significant" Stellar Wind contributions to FBI counterterrorism efforts.[455] The FBI OGC told us that

---

[454] As we described earlier in this chapter, the FBI considered a tipper "significant" if it led to any of three investigative results: the identification of a terrorist, the deportation from the United States of a suspected terrorist, or the development of an asset that can report about the activities of terrorists. ~~(S//NF)~~

[455] As described earlier in this chapter, the FBI considered a tipper "significant" if it led to any of three investigative results: the identification of a terrorist, the deportation from the United States of a suspected terrorist, or the development of an asset that can report about the activities of terrorists. ~~(TS//NF)~~

statements by senior FBI officials in congressional testimony that the Stellar Wind program had value were based in part on the results of the first study, which found that 1.2 percent of the Stellar Wind leads made significant contributions to FBI cases. ~~(TS//STLW//SI//OC/NF)~~

FBI agents we interviewed generally were supportive of Stellar Wind (or [redacted]), calling the information "one tool of many" in the FBI's anti-terrorism efforts that "could help move cases forward" by, for example, confirming a subject's contacts with individuals involved in terrorism or identifying additional terrorist contacts. However, FBI agents and analysts also told us that the Stellar Wind information disseminated to FBI field offices could also be frustrating because it often lacked details about the foreign individuals allegedly involved in terrorism with whom domestic telephone numbers and e-mail addresses were in contact. Some agents also believed that the [redacted] project failed to adequately prioritize leads sent to FBI field offices. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

FBI Director Mueller told us that he believes the Stellar Wind program was useful and that the FBI must follow every lead it receives in order to prevent future terrorist attacks. He stated that to the extent such information can be gathered and used legally it must be exploited, and that he "would not dismiss the potency of a program based on the percentage of hits." Other witnesses shared this view that an intelligence program's value cannot be assessed by statistical measures alone. General Hayden said that the value of the program may lie in its ability to help the Intelligence Community determine that the terrorist threat embedded within the country is not as great as once feared. Some witnesses also believed that the value of the program should not depend on documented "success stories," but rather on maintaining an intelligence capability to detect potential terrorist activity in the future. Several witnesses suggested that the program provides an "early warning system" to allow the Intelligence Community to detect potential terrorist attacks, even if the system has not specifically uncovered evidence of preparations for such an attack.
~~(TS//STLW//SI//OC/NF)~~

As part of our analysis, we sought to look beyond these comments of general support for Stellar Wind to specific, concrete examples of the program's contributions that illustrated the role Stellar Wind information either has or could play in the FBI's counterterrorism efforts. We examined five cases frequently cited in documents we reviewed and during our interviews as examples of Stellar Wind's positive contributions to the FBI's counterterrorism efforts. The evidence indicated that Stellar Wind information had value in some of these investigations by causing the FBI to take action that led to useful investigative results. In other cases the connection between the Stellar Wind information and the FBI's investigative actions was more difficult to discern. ~~(TS//STLW//SI//OC/NF)~~

In the end, we found it difficult to assess or quantify the overall effectiveness of the Stellar Wind program to the FBI's counterterrorism activities. However, based on the interviews conducted and documents reviewed, we concluded that although Stellar Wind information had value in some counterterrorism investigations, it generally played a limited role in the FBI's overall counterterrorism efforts. ~~(S//NF)~~

It is also important to note that a significant consequence of the NSA program and the FBI's approach to assigning leads for program information was that FBI field offices conducted many threat assessments on individuals located in the United States, including U.S. persons, that typically were determined not to have any nexus to terrorism or represent a threat to national security. As a result, the FBI collected and retained a significant amount of personal information about the users of tipped telephone numbers and e-mail addresses, such as names and home addresses, places of employment, foreign travel, and the identity of family members. The results of these threat assessments and the information collected generally were reported in communications to FBI Headquarters and uploaded into FBI databases. ~~(TS//STLW//SI//OC/NF)~~

The FBI's collection of information in this manner is ongoing under [redacted] project, the successor FBI project to [redacted] which disseminates to FBI field offices lead information the NSA derives from bulk telephony and e-mail meta data now collected under FISA authority. Like [redacted] project requires FBI field offices to conduct threat assessments on telephone numbers and e-mail addresses identified through the NSA's analytical process that the FBI is not already aware of, including telephone numbers and e-mail addresses one or two steps removed from direct contacts with individuals involved in terrorism. To the extent the leads derived from the FISA-authorized activities generate results similar to those under Stellar Wind, the FBI threat assessments will continue to result in the collection and retention of a significant amount of personal information about individuals in the United States, including U.S. persons, who do not have a nexus to terrorism or represent a threat to national security. ~~(TS//STLW//SI//OC/NF)~~ b1, b3, b7E

We recommend that, as part of the [redacted] project, the Justice Department's National Security Division (NSD), working with the FBI, should collect information about the quantity of telephone numbers and e-mail addresses disseminated to FBI field offices that are assigned as Action leads and that require offices to conduct threat assessments. The information compiled by the Justice Department should include whether individuals identified in threat assessments are U.S. or non-U.S. persons and whether the threat assessments led to the opening of preliminary or full national security investigations. With respect to threat assessments that conclude that users of tipped telephone numbers or e-mail addresses are b1, b3, b7E

not involved in terrorism and are not threats to national security, the Justice Department should take steps to track the quantity and nature of the U.S. person information collected and how the FBI retains and utilizes this information. This will enable the Justice Department and entities with oversight responsibilities, including the OIG and congressional committees, to assess the impact this intelligence program has on the privacy interests of U.S. persons and to consider whether, and for how long, such information should be retained. ~~(TS//SI//NF)~~

We also recommend that, consistent with NSD's current oversight activities and as part of its periodic reviews of national security investigations at FBI Headquarters and field offices, NSD should review a representative sampling [redacted] leads to those offices. For each lead examined, NSD should assess FBI compliance with applicable legal requirements in the use of the lead and in any ensuing investigations, particularly with the requirements governing the collection and use of U.S. person information. ~~(TS//SI//NF)~~ b1, b3, b7E

VI. Discovery and "Scrubbing" Issues ~~(TS//SI//NF)~~

Although Stellar Wind was conceived and implemented as an intelligence-gathering program, it was inevitable that the information from this program would intersect with the Department's prosecutorial functions, both in criminal cases brought in federal courts and in seeking FISA orders from the FISA Court. We found that the limited number of Department read-ins also had adverse consequences on issues related to these Department functions. ~~(TS//STLW//SI//OC/NF)~~

One such issue concerned the Department's compliance with discovery obligations in international terrorism prosecutions, which we discuss in Chapter Seven. We determined that the Department was aware as early as [redacted] that information collected under Stellar Wind could have implications for the Department's litigation responsibilities under Federal Rule of Criminal Procedure 16 and *Brady v. Maryland*, 373 U.S. 83 (1963). ~~(TS//STLW//SI//OC/NF)~~ b1, b3

Analysis of this discovery issue was first assigned to John Yoo in [redacted] Yoo, working alone, produced a legal analysis of the government's discovery obligations in the case of [redacted] (b) (5), (b)(3), (b)(1) and [redacted] (b) (5), (b)(3), (b)(1) b1, b3, b6, b7C, b7E

(b) (5)

b1, b3, b6, b7C, b7E

~~(TS//STLW//SI//OC/NF)~~

[redacted]

No Justice Department attorneys with terrorism prosecution responsibilities were read into the Stellar Wind program until mid-2004, and as a result the Department continued to lack the advice of attorneys who were best equipped to identify and examine the discovery issues in connection with the program. Since that time the Department has taken steps to respond, on a case-by-case basis, to [redacted] discovery motions

(b)(1), (b)(3)

[redacted] These responses involve the use of the Classified Information Procedures Act, 18 U.S.C. App. 3, to file *ex parte* in camera pleadings with federal courts to describe any potentially responsive Stellar Wind-derived information.

(b)(1), (b)(3)

[redacted]

[redacted] ~~(TS//STLW//SI//OC/NF)~~

However, the Department of Justice continues to lack a comprehensive process for identifying potentially discoverable Stellar Wind information in terrorism cases. In this regard, we recommend that the Department assess its discovery obligations regarding Stellar Wind-derived information in international terrorism prosecutions. We also recommend that the Department carefully consider whether it must re-examine past cases to see whether potentially discoverable but undisclosed Rule 16 or *Brady* material was collected by the NSA under the program, and take appropriate steps to ensure that it has complied with its discovery obligations in such cases. We also recommend that the Department, in coordination with the NSA, implement a procedure to identify Stellar Wind-derived information that may be associated with international terrorism cases currently pending or likely to be brought in the future and evaluate whether such information should be disclosed in light of the

government's discovery obligations under Rule 16 and *Brady*. ~~(TS//STLW//SI//OC/NF)~~

In addition, we examined the issue of the Department's use of Stellar Wind-derived information in FISA applications. We believe it was foreseeable that some Stellar Wind-derived information would be contained in the FISA applications filed by the Department's Office of Intelligence Policy and Review (OIPR). OIPR Counsel Baker believed, and we agree, that it would have been detrimental to this relationship if the Court learned that information from Stellar Wind was included in FISA applications without the Court being told so in advance. As discussed in Chapter Three, White House officials initially rejected the idea of reading in members of the FISA Court, but after Department officials continued to press the issue, ultimately in January 2003 agreed to read in a single judge in January 2002 (Presiding Judge Lamberth, followed by Presiding Judge Kollar-Kotelly in May 2002). ~~(TS//STLW//SI//OC/NF)~~

The "scrubbing" procedures imposed by the Court and implemented by Baker to account for Stellar Wind-derived information in international terrorism FISA applications created concerns among some OIPR attorneys about the unexplained changes being made to their FISA applications. These scrubbing procedures also substantially altered the assignment of cases to FISA Court judges for nearly 3 years. We concluded that once Stellar Wind began to affect the functioning of the FISA process shortly after the program's inception, the number of OIPR staff and FISA Court judges read into Stellar Wind should have increased. Instead, read-ins were limited to a single OIPR official for over two years and to the Presiding Judge of the FISA Court for a period of four years. ~~(TS//STLW//SI//OC/NF)~~

The Justice Department, together with the FBI and the NSA, today continues to apply scrubbing procedures to international terrorism FISA applications. Since January 2006, all members of the Court have been briefed on the Stellar Wind program and all of the judges handle applications that involve Stellar Wind-derived information in FISA applications. While we found that the government has expended considerable resources to comply with the scrubbing procedures required by the FISA Court since February 2002, we did not find any instances of the government being unable to obtain FISA surveillance coverage on a target because of this requirement. ~~(TS//STLW//SI//OC/NF)~~

VII. Gonzales's Statements (U)

As part of this review, the OIG examined whether Attorney General Gonzales made false or misleading statements to Congress related to the Stellar Wind program. We concluded that Gonzales's testimony did not

constitute a false statement and that he did not intend to mislead Congress. However, we concluded that his testimony in several respects was confusing, not accurate, and had the effect of misleading those who were not knowledgeable about the program. ~~(S//NF)~~

Aspects of the Stellar Wind program were first disclosed publicly in a series of articles in The New York Times in December 2005. In response, the President publicly confirmed a portion of the program – which he called the terrorist surveillance program – describing it as the interception of the content of international communications of people reasonably believed to have links to al Qaeda and related organizations (basket 1). Subsequently, Attorney General Gonzales was questioned about NSA surveillance activities in two hearings before the Senate Judiciary Committee in February 2006 and July 2007. ~~(TS//STLW//SI//OC/NF)~~

Through media accounts and former Deputy Attorney General Comey's Senate Judiciary Committee testimony in May 2007, it was publicly revealed that the Department and the White House had a major disagreement related to the program in March 2004. As discussed in Chapter Four, this dispute – which resulted in the visit to Attorney General Ashcroft's hospital room by Gonzales and Card and brought several senior Department and FBI officials to the brink of resignation after the White House continued the program [redacted] ~~(TS//STLW//SI//OC/NF)~~

In his testimony before the Senate Judiciary Committee, Gonzales stated that the dispute at issue between the Department and the White House did not relate to the "Terrorist Surveillance Program" that the President had confirmed, but rather pertained to other intelligence activities. We believe this testimony created the misimpression that the dispute concerned activities entirely unrelated to the terrorist surveillance program, which was not accurate. In addition, we believe Gonzales's testimony that Department attorneys did not have "reservations" or "concerns" about the program the "President has confirmed" was incomplete and confusing because Gonzales did not account for the fact that the Department's concerns were what led to [redacted] and that these concerns had been conveyed to the White House over a period of months prior to and including March 2004 when the issue was resolved. ~~(S//NF)~~

We recognize that Attorney General Gonzales was in the difficult position of testifying about a highly classified program in an open forum. However, we also believe that Gonzales, as a participant in the March 2004 dispute between the White House and the Justice Department and, more importantly, as the nation's chief law enforcement officer, had a duty to balance his obligation not to disclose classified information with the need

not to be misleading in his testimony about the events that nearly led to mass resignations of the most senior officials at the Justice Department and the FBI. Although we believe that Gonzales did not intend to mislead Congress, we believe his testimony was confusing, inaccurate, and had the effect of misleading those who were not knowledgeable about the program. ~~(TS//SI//NF)~~

VIII. Conclusion (U)

From the inception of the Stellar Wind program in October 2001, vast amounts of information about telephone and e-mail communications were collected and stored in databases at the NSA. The NSA used this information to conduct analysis and disseminate reports to support the government's counterterrorism efforts. We found that in the early years of the Stellar Wind program, the Department of Justice lacked the necessary legal resources to carry out an adequate review of the legality of the program. The White House strictly controlled the Department's access to the program. For the first year and a half of the program only 3 Department officials were read into Stellar Wind, and only 3 more officials had been read in by the end of 2003. Only a single Department attorney analyzed the legal basis for the program during its first year and a half of its operation. Beginning in mid-2003, after additional Department officials were read into the program, the Department determined that this attorney's initial legal analysis was legally and factually flawed. ~~(TS//STLW//SI//OC/NF)~~

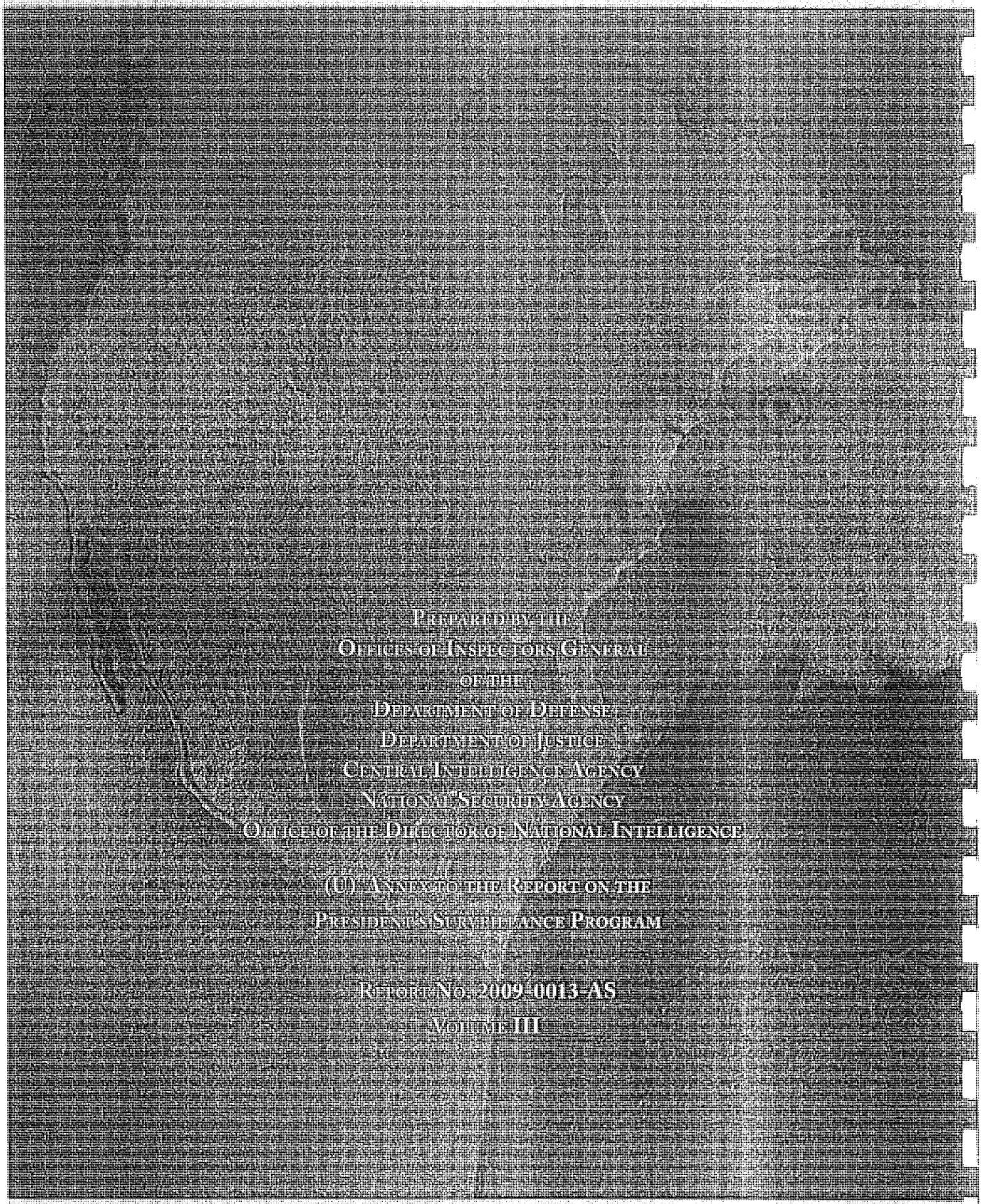
We believe that the strict controls over the Department's access to the program undermined the role of the Justice Department in advising the President as to the legality of the program during its early phase of operation. The Department's comprehensive reassessment of the program's legality beginning in mid-2003 resulted in a contentious dispute with the White House that nearly led to the mass resignation of the Department's senior leadership. In March 2004 the White House continued the program despite the Department's conclusion that it found no legal support for aspects of the program. In the face of the potential resignations, however, the White House [redacted] in accord with the Department's legal concerns. Eventually, the entire program was transitioned, in stages, to the authority of the FISA statute. ~~(TS//STLW//SI//OC/NF)~~

Given the broad nature of the collection activities under the Stellar Wind program, the substantial amount of information the program collected related to U.S. persons, and the novel legal theories advanced to support the program, we believe that the Department should have more carefully and thoroughly reviewed the legality of the program, in accord with its normal

peer review and oversight practices, particularly during its first year and a half of operation. ~~(TS//STLW//SI//OC/NF)~~

We also concluded that the Department should have begun efforts to transition the Stellar Wind program to FISA authority earlier than March 2004, when that process began, especially as Stellar Wind became less a temporary response to the September 11 attacks and more a permanent surveillance tool. We believe that such broad surveillance and collection activities conducted in the United States that impact U.S. persons, particularly when they extend for such a significant period of time, should be conducted pursuant to statute and be subjected to judicial oversight. Placing such activities under Court supervision, as now occurs, also provides an important measure of accountability for the government's conduct that is less assured when the activities are authorized and supervised by the Executive Branch alone. ~~(TS//STLW//SI//OC/NF)~~

Finally, we believe that the Department should carefully monitor the collection, use, and retention of the information that is now collected under FISA authority, given the expansive scope of the collection activities. The Department and other agencies should also continue to examine the value of collecting such information to the government's ongoing counterterrorism efforts. ~~(TS//SI//NF)~~



Prepared by the
Offices of Inspectors General
of the
Department of Defense
Department of Justice
Central Intelligence Agency
National Security Agency
Office of the Director of National Intelligence

(U) Annex to the Report on the President's Surveillance Program

Report No. 2009-0013-AS

Volume III

(U) REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

VOLUME I

10 JULY 2009

PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Special Warning

The report contains compartmented, classified material and no secondary distribution may be made without prior consent of the participating Inspectors General. Improper disclosure of this report may result in criminal, civil, or administrative penalties.

REPORT NO. 2009-0013-A

APPROVED FOR PUBLIC RELEASE

10 July 2009

(U) Preface

(U) Title III of the Foreign Intelligence Surveillance Act Amendments Act of 2008 required the Inspectors General (IGs) of the elements of the Intelligence Community that participated in the President's Surveillance Program (PSP) to conduct a comprehensive review of the Program. The IGs of the Department of Justice (DoJ), the Department of Defense (DoD), the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Office of the Director of National Intelligence (ODNI) participated in the review required under the Act. The Act required the IGs to submit a comprehensive report on the review to the Senate Select Committee on Intelligence, the Senate Committee on the Judiciary, the House Permanent Select Committee on Intelligence, and the House Committee on the Judiciary.

(U) Because many aspects of the PSP remain classified, and in order to provide the Congressional committees the complete results of our review, we have prepared this classified report on the PSP. The report is in three volumes:

- Volume I summarizes the collective results of the IGs' review.
- Volume II contains the individual reports prepared and issued by the DoD, CIA, NSA, and ODNI IGs.
- Volume III contains the report prepared and issued by the DoJ IG.

(U) The unclassified report on the PSP required by Title III has been provided to the Congressional committees in a separately bound volume.

Unclassified When Separated
From Attachment

~~Derived From: NSA/CSSM 1-52, 2-400,~~
~~NSA/CSS M 1-52, 12-48~~
~~Dated: 20070108~~
~~Declassify On: 20340713~~

APPROVED FOR PUBLIC RELEASE

APPROVED FOR PUBLIC RELEASE

Glenn A. Fine
Inspector General
Department of Justice

Gordon S. Heddell
Acting Inspector General
Department of Defense

Patricia A. Lewis
Acting Inspector General
Central Intelligence Agency

George Ellard
Inspector General
National Security Agency

Roslyn A. Mazer
Inspector General
Office of the Director of
National Intelligence

APPROVED FOR PUBLIC RELEASE

(U) Table of Contents

(U) INTRODUCTION 1
(U) Scope of the Review 1
(U) Methodology 2
(U) INCEPTION OF THE PRESIDENT'S SURVEILLANCE PROGRAM 4
(U) National Security Agency Counterterrorism Efforts Prior to 11 September 2001 4
(U) NSA Initially Used Existing Authorities to Enhance Signals Intelligence (SIGINT) Collection After the September 2001 Terrorist Attacks 5
(U) NSA Explored Options to Improve SIGINT Collection and Address Intelligence Gaps on Terrorist Targets 6
(U) Impediments to SIGINT Collection Against Terrorist Targets Were Discussed With the White House 7
(U) Authorization of the President's Surveillance Program 7
(U) SIGINT Activities Authorized Under the Program 7
(U) Content of the Presidential Authorizations and Department of Justice Certification as to Form and Legality 9
(U) The Threat Assessment Memorandums Supporting Presidential Authorization of the Program 10
(U) Early Revisions to the Presidential Authorizations 11
(U) DoJ Office of Legal Counsel Memorandums Supporting Legality of the Program 12
(U) IMPLEMENTATION OF THE PRESIDENT'S SURVEILLANCE PROGRAM 16
(U) NSA Implementation 16
[redacted] 17

~~(TS//SI//NF)~~ Telephone and Internet Communications Content Collection and Analysis 18

~~(TS//SI//NF)~~ Telephony and Internet Metadata Collection and Analysis 20

(U) NSA Reporting From the President's Surveillance Program 21

(U) NSA Managerial Structure and Oversight of the President's Surveillance Program 22

(U) NSA Management Controls to Ensure Compliance With Presidential Authorizations 23

(U) NSA Inspector General Oversight of the Program 24

(U) Access to the President's Surveillance Program 25

(U) Congressional Briefings on the Program 26

(U) Foreign Intelligence Surveillance Court Briefings on the Program 27

(U) FBI Participation in the President's Surveillance Program 28

(U) CIA Participation in the President's Surveillance Program 30

(U) NCTC Participation in the President's Surveillance Program 32

(U) The President's Surveillance Program and the Foreign Intelligence Surveillance Court 33

(U) Discovery Issues Associated With the President's Surveillance Program 35

(U) LEGAL REASSESSMENT OF THE PRESIDENT'S SURVEILLANCE PROGRAM (2003 – 2004) 36

~~(TS//SI//NF)~~ Concern Over the [redacted] Collection 36

(U) A New Legal Basis for the Program Is Adopted 37

(U) Department of Justice Officials Convey Concerns About the Program to the White House 39

(U) Conflict Between the Department of Justice and the White House Over the Program 40

~~(S//NF)~~ White House Counsel Certifies Presidential Authorization Without Department of Justice Concurrence 44

~~(TS//SI//NF)~~ White House Agrees to [redacted] 48

(U) Restrictions on Access to the President's Surveillance Program Impeded Department of Justice Legal Review 50

(U) TRANSITION OF PRESIDENT'S SURVEILLANCE PROGRAM ACTIVITIES TO FOREIGN INTELLIGENCE SURVEILLANCE ACT AUTHORITY 50

~~(TS//SI//NF)~~ Internet Metadata Collection Transition to Operation Under FISA Authority 50

(U) Department of Justice Notices of Compliance Incidents 53

~~(TS//SI//NF)~~ Telephony Metadata Collection Transition to Operation Under FISA Authority 54

~~(TS//SI//NF)~~ Content Collection Transition to Operation Under FISA Authority 57

(U) IMPACT OF THE PRESIDENT'S SURVEILLANCE PROGRAM ON INTELLIGENCE COMMUNITY COUNTERTERRORISM EFFORTS 60

(U) Senior Intelligence Community Officials Believe That the President's Surveillance Program Filled an Intelligence Gap 60

(U) Difficulty in Assessing the Impact of the President's Surveillance Program 61

(U) Impact of the President's Surveillance Program on FBI Counterterrorism Efforts 61

(U) FBI Efforts to Assess the Value of the Program 62

(U) FBI Judgmental Assessments of the Program 62

(U) Impact of the President's Surveillance Program on CIA Counterterrorism Operations 63

(U) The CIA Did Not Systematically Assess the Effectiveness of the Program 63

(U) Several Factors Hindered CIA Utilization of the Program 64

(U) Impact of the President's Surveillance Program on NCTC Counterterrorism Efforts 65

(U) Counterterrorism Operations Supported by the President's Surveillance Program 65

(U) ATTORNEY GENERAL GONZALES'S TESTIMONY ON THE PRESIDENT'S SURVEILLANCE PROGRAM 68

(U) CONCLUSIONS 69

(U) The President's Surveillance Program

(U) INTRODUCTION

~~(TS//SI//OC/NF)~~ In response to the terrorist attacks of 11 September 2001, on 4 October 2001, President George W. Bush issued a Top Secret authorization to the Secretary of Defense directing that the signals intelligence (SIGINT) capabilities of the National Security Agency (NSA) be used to detect and prevent further attacks in the United States. The Presidential Authorization stated that an extraordinary emergency existed permitting the use of electronic surveillance within the United States for counterterrorism purposes, without a court order, under certain circumstances. For more than five years, the Presidential Authorization was renewed at 30- to 60-day intervals to authorize the highly classified NSA surveillance program, which is referred to throughout this report as the President's Surveillance Program (PSP).[1]

~~(TS//SI//OC/NF)~~ Under the Presidential Authorizations, the NSA intercepted the content of international telephone and Internet communications of both U.S. and non-U.S. persons. In addition, the NSA collected telephone and Internet metadata—communications signaling information showing contacts between and among telephone numbers and Internet communications addresses, but not including the contents of the communications. [redacted] The content and metadata information was analyzed by the NSA, working with other members of the Intelligence Community (IC), to generate intelligence reports. These reports were sent to the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and other intelligence organizations.

(U) The scope of collection permitted under the Presidential Authorizations varied over time. In stages between July 2004 and January 2007, NSA ceased PSP collection activities under Presidential authorization and resumed them under four separate court orders issued in accordance with the Foreign Intelligence Surveillance Act of 1978 as amended (FISA).[2]

(U) Scope of the Review

(U) Title III of the Foreign Intelligence Surveillance Act Amendments Act of 2008 (FISA Amendments Act)—signed into law on 10 July 2008—required the inspectors

---

[1] ~~(S//NF)~~ The cover term NSA uses to protect the President's Surveillance Program is STELLARWIND.

[2] (U) Unless otherwise indicated, references to FISA in this report are to the statute as it existed prior to being amended in 2008.

general of the elements of the IC that participated in the PSP to conduct a comprehensive review of the program.[3] The Act required that the review examine:

> (A) all of the facts necessary to describe the establishment, implementation, product, and use of the product of the Program;
>
> (B) access to legal reviews of the Program and access to information about the Program;
>
> (C) communications with, and participation of, individuals and entities in the private sector related to the Program;
>
> (D) interaction with the Foreign Intelligence Surveillance Court and transition to court orders related to the Program; and
>
> (E) any other matters identified by any such Inspector General that would enable that Inspector General to complete a review of the Program, with respect to such Department or element.

(U) The Inspectors General (IGs) of the Department of Defense (DoD), the Department of Justice (DoJ), the CIA, the NSA, and the Office of the Director of National Intelligence (ODNI) conducted the review required under the Act. This report summarizes the collective results of the IGs' review. Conclusions and recommendations in this report that are attributed to a particular IG should be understood to represent that IG's opinion. Individual reports detail the results of each IG's review and are annexes to this report. All of the reports have been classified in accordance with the program's classification guide, which was revised during our review and re-issued on 21 January 2009.

(U) Title III of the FISA Amendments Act also required that the report of any investigation of matters relating to the PSP conducted by the DoJ, Office of Professional Responsibility (OPR) be provided to the DoJ IG, and that the findings and conclusions of such investigation be included in the DoJ IG's review. OPR intends to review whether any standards of professional conduct were violated in the preparation of the first series of legal memorandums supporting the PSP. OPR has not yet completed its review or provided its findings and conclusions to the DoJ IG.

(U) Methodology

(U) During the course of this review, the participating IGs conducted approximately 200 interviews. Among the individuals we interviewed were: former White House Counsel and Attorney General Alberto R. Gonzales; former Deputy Attorney General James B. Comey; FBI Director Robert S. Mueller, III; former Secretary of Defense

---

[3] (U) The President's Surveillance Program is defined in the Act as the intelligence activity involving communications that was authorized by the President during the period beginning on 11 September 2001 and ending on 17 January 2007, including the program referred to by the President in a radio address on 17 December 2005 (commonly known as the Terrorist Surveillance Program).

Donald H. Rumsfeld; former NSA Director, Principal Deputy Director of National Intelligence, and CIA Director Michael V. Hayden; former Director of Central Intelligence (DCI) and CIA Director Porter J. Goss; NSA Director Lieutenant General Keith B. Alexander; former Directors of National Intelligence John D. Negroponte and J. M. McConnell; and former National Counterterrorism Center (NCTC) Director John O. Brennan. Certain other persons who had significant involvement in the PSP either declined or did not respond to our requests for an interview, including former Deputy Secretary of Defense Paul D. Wolfowitz; former Chief of Staff to President Bush Andrew H. Card; David S. Addington, former Counsel to Vice President Richard B. Cheney; former Attorney General John D. Ashcroft; former Deputy Assistant Attorney General John Yoo; and former DCI George J. Tenet.

~~(S//NF)~~ We interviewed former NSA [redacted] as well as leadership [redacted] within the NSA Signals Intelligence Directorate (SID). We interviewed personnel from the CIA [redacted]; senior FBI Counterterrorism Division officials; FBI special agents and intelligence analysts; senior officials from DoJ's Criminal and National Security Divisions; and current and former senior NCTC officials. We also interviewed DoJ officials and office of general counsel officials from the participating organizations who were involved in legal reviews of the PSP and/or had access to the memorandums supporting the legality of the PSP.

~~(S//NF)~~ We examined thousands of electronic and hardcopy documents, including the Presidential Authorizations, terrorist threat assessments, legal memorandums, applicable regulations and policies, briefings, reports, correspondence, and notes. We obtained access to an FBI database of PSP-derived leads that had been disseminated to FBI field offices. We used the database to confirm information obtained through interviews and to assist in our analysis of FBI investigations that utilized PSP information. We evaluated the justifications included in the requests for information (RFIs) submitted by the CIA to the NSA to determine whether they were in accordance with program guidelines. Reports of prior reviews and investigations of the PSP conducted by the NSA IG were also utilized in our review.

[redacted]

(U) INCEPTION OF THE PRESIDENT'S SURVEILLANCE PROGRAM

(U) National Security Agency Counterterrorism Efforts Prior to 11 September 2001

~~(C//NF)~~ For more than a decade before the terrorist attacks of 11 September 2001, NSA was applying its SIGINT capabilities against terrorist targets in response to IC requirements.[1] The NSA, SID, Counterterrorism (CT) Product Line led these efforts. NSA was authorized by Executive Order (E.O.) 12333, *United States Intelligence Activities*, 4 December 1981, as amended, to collect, process, and disseminate SIGINT information for foreign intelligence and counterintelligence purposes in accordance with DCI guidance and to support the conduct of military operations under the guidance of the Secretary of Defense. It is the policy of U.S. Government entities that conduct SIGINT activities that they will collect, retain, and disseminate only foreign communications. In September 2001, NSA's compliance procedures defined foreign communications as communications having at least one communicant outside the United States, communications entirely among foreign powers, or communications between a foreign power and officers or employees of a foreign power. All other communications were considered domestic communications. NSA was not authorized under E.O. 12333 to collect communications from a wire in the United States without a court order unless the communications originated and terminated outside the United States or met applicable exceptions to the requirement of a court order under FISA.

(U) FISA, 50 U.S.C. § 1801, et seq., was enacted in 1978 to "provide legislative authorization and regulation for all electronic surveillance conducted within the United States for foreign intelligence purposes." FISA authorizes the Federal Government to engage in electronic surveillance and physical searches, to use pen register and trap and trace devices, and to obtain business records to acquire foreign intelligence information by targeting foreign powers and agents of foreign powers inside the United States.[4] As a general rule, the FISC must first approve an application for a warrant before the government may initiate electronic surveillance.

~~(S//SI//NF)~~ Prior to the PSP, NSA authority to intercept foreign communications included the Director, NSA's authority to approve the targeting of communications with one communicant within the United States if technical devices could be employed to limit collection to communications where the target is a non-U.S. person located outside the United States, [redacted]

[4] (U) The term "pen register" is defined in 18 U.S.C. § 3127 as a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication. The term "trap and trace device" is defined in 18 U.S.C. § 3127 as a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

[redacted] If technical devices could not be used to limit collection, the collection required approval by the Attorney General. The Director, NSA could exercise this authority, except when the collection was otherwise regulated, for example, under FISA for communications collected from a wire in the United States.

(U) NSA Initially Used Existing Authorities to Enhance Signals Intelligence (SIGINT) Collection After the September 2001 Terrorist Attacks

~~(TS//SI//NF)~~ On 14 September 2001, NSA Director Hayden used his E.O. 12333 authority to approve a SID CT Product Line request to target [redacted] foreign telephone numbers [redacted] He approved the tasking of the specified numbers, or selectors. This was an aggressive use of authority because of [redacted] Hayden's 14 September 2001 approval memorandum stated that the purpose of the targeting was to facilitate "dialing analysis/contact chaining."[5] NSA Office of General Counsel (OGC) personnel concurred with the proposed activity, but provided a handwritten note to Hayden stating that chaining was permitted only on foreign numbers, and no U.S. number could be chained without a court order. Collection of the content [redacted] was not addressed in the memorandum. However, other documentation indicates that NSA OGC and SID personnel understood that Hayden also had approved content collection and analysis. NSA OGC personnel told us that Hayden's action was a lawful exercise of his authority under E.O. 12333. In addition, according to NSA's Deputy General Counsel, Hayden had decided by 26 September 2001 that [redacted] would be presumed to be of foreign intelligence value and could be provided to the FBI. Hayden told us that his actions were a "tactical decision" and that he was operating in a unique environment because it was widely believed that more terrorist attacks on U.S. soil were imminent.

~~(S//NF)~~ In late September, Hayden informed Tenet that he had expanded SIGINT operations under E.O. 12333 authority. According to Hayden, Tenet later said that he had explained the NSA's expanded SIGINT operations to Vice President Cheney during a meeting at the White House. On 2 October 2001, Hayden briefed the House Permanent Select Committee on Intelligence on his decision to expand operations under E.O. 12333 and informed members of the Senate Select Committee on Intelligence by telephone.

---

5 ~~(S//SI//NF)~~ Dialing analysis/contact chaining is the process of [redacted] from the communications sent or received by targeted entities.

(U) NSA Explored Options to Improve SIGINT Collection and Address Intelligence Gaps on Terrorist Targets

~~(S//NF)~~ Hayden did not attend the meeting at the White House at which Tenet explained the NSA's expanded SIGINT operations to the Vice President. According to Hayden, Tenet told him that during the meeting the Vice President asked if the IC was doing everything possible to prevent another attack. The Vice President specifically asked Tenet if NSA could do more. Tenet then discussed the matter with Hayden. Hayden told Tenet that nothing more could be done within existing authorities. In a follow-up telephone conversation, Tenet asked Hayden what the NSA could do if it was provided additional authorities. To formulate a response, Hayden met with NSA personnel, who were already working to fill intelligence gaps, to identify additional authorities to support SIGINT collection activities that would be operationally useful and technically feasible. In particular, discussions focused on how NSA might bridge the "international gap," i.e., collection of international communications in which one communicant was within the United States.

(U) In the days immediately after 11 September 2001, the House Permanent Select Committee on Intelligence asked NSA for technical assistance in drafting a proposal to amend FISA to give the President authority to conduct electronic surveillance without a court order to obtain foreign intelligence information. On 20 September 2001, the NSA General Counsel wrote to White House Counsel Gonzales asking if the proposed amendment to FISA had merit. We found no record of a response to the NSA General Counsel's writing and could not determine why the proposal to amend FISA was not pursued at that time.

(U) Hayden said that, in his professional judgment, NSA could not address the intelligence gap using FISA. The process for obtaining FISC orders was slow; it involved extensive coordination and separate legal and policy reviews by several agencies. Although FISA's emergency authorization provision permitted 72 hours of surveillance before obtaining a court order, it did not allow the government to undertake surveillance immediately. Rather, the Attorney General had to ensure that emergency surveillance would satisfy the standards articulated in FISA and be acceptable to the FISC.

[redacted]

[redacted]

(U) Impediments to SIGINT Collection Against Terrorist Targets Were Discussed With the White House

~~(S//NF)~~ Hayden recalled that, after consulting with NSA personnel, he discussed with the White House how FISA constrained NSA collection of communications carried on a wire in the United States. Hayden explained that NSA could not collect from a wire in the United States, without a court order, content or metadata from communications that originated and/or terminated in the United States. Hayden also said that communications metadata do not have the same level of constitutional protection as the content of communications and that access to metadata concerning communications having one end in the United States would significantly enhance NSA's analytic capabilities. Hayden suggested that the ability to collect communications that originated or terminated in the United States without a court order would increase NSA's speed and agility. After two additional meetings with Vice President Cheney to discuss further how NSA collection capabilities could be expanded along the lines described at the White House meeting, the Vice President told Hayden to work out a solution with Counsel to the Vice President David Addington.

(U) Authorization of the President's Surveillance Program

~~(TS//SI//NF)~~ According to Hayden, Addington drafted the first Presidential Authorization of the PSP. Hayden characterized himself as the "subject matter expert," and he said that no other NSA personnel, including the General Counsel, participated in drafting the authorization. Hayden also said that DoJ personnel had not been involved in his discussions with Addington concerning Presidential authorization of the PSP. The PSP came into existence on 4 October 2001, when President Bush signed the Presidential Authorization drafted by Addington. The authorization was entitled: *Presidential Authorization for Specified Electronic Surveillance Activities during a Limited Period to Detect and Prevent Acts of Terrorism within the United States*. Between 4 October 2001 and 8 December 2006, President Bush signed 43 authorizations, exclusive of modifications and other program-related memoranda to the Secretary of Defense.

(U) SIGINT Activities Authorized Under the Program

~~(TS//STLW//SI//OC/NF)~~ The 4 October 2001 Presidential Authorization directed the Secretary of Defense to [redacted]

[redacted]

~~(TS//STLW//SI//OC/NF)~~ The first Presidential Authorization allowed NSA to intercept the content of [redacted] any communication, including those to, from, or exclusively within the United States, where probable cause existed to believe one of the communicants was engaged in international terrorism. The authorization also allowed the NSA to acquire telephony and Internet metadata where one end of the communication was outside the United States or neither communicant was known to be a U.S. citizen. For telephone calls, metadata generally referred to "dialing-type information" (the originating and terminating telephone numbers, and the date, time, and duration of the call), but not the content of the call. For Internet communications, metadata generally referred to the "to," "from," "cc," "bcc," and "sent" lines of a message, but not the "subject" line or content. [redacted]

~~(TS//STLW//SI//OC/NF)~~ The Secretary of Defense directed NSA, in writing, on 8 October 2001 to execute the authorization to conduct specified electronic surveillance on targets related to [redacted] international terrorism.[6] Because the surveillance was conducted in the United States, included [redacted] communications into or out of the United States, and a subset of these communications was to or from persons in the United States, the surveillance otherwise would have required a FISC order. NSA was also allowed to retain, process, analyze, and disseminate intelligence from communications acquired under the Presidential Authorization.

~~(TS//STLW//SI//OC/NF)~~ In addition to allowing the interception of the content of communications into or out of the United States, paragraph (a)(ii) of the first Presidential Authorization allowed NSA to intercept the content of purely domestic communications. Hayden told us he did not realize this until Addington specifically raised the subject during

---

6 [redacted]

a meeting to discuss renewing the authorization. According to Hayden, he told Addington that NSA would not collect domestic communications because NSA is a foreign intelligence agency, its infrastructure did not support domestic collection, and he would require such a high evidentiary standard to justify intercepting purely domestic communication that such cases might just as well go to the FISC.

(U) Content of the Presidential Authorizations and Department of Justice Certification as to Form and Legality

~~(S//NF)~~ Each of the Presidential Authorizations included a finding to the effect that terrorist groups of global reach possessed the intent and capability to attack the United States, that an extraordinary emergency continued to exist, and that these circumstances constituted an urgent and compelling governmental interest permitting electronic surveillance within the United States for counterterrorism purposes, without judicial warrants or court orders. The primary authorities cited for the legality of the electronic surveillance and related activities were Article II of the Constitution and the 18 September 2001 Authorization for Use of Military Force Joint Resolution (AUMF).

[redacted] The President also noted his intention to inform appropriate members of the Senate and the House of Representatives of the program "as soon as I judge that it can be done consistently with national defense needs."

~~(S//NF)~~ Ashcroft certified the first Presidential Authorization as to "form and legality" on 4 October 2001. According to NSA records, this was the same day that Ashcroft was read into the PSP. There was no legal requirement that the Presidential Authorizations of the PSP be certified by the Attorney General or other DoJ officials. Former senior DoJ official Patrick F. Philbin told us he thought one purpose of the certification was to give the program a sense of legitimacy so that it not "look like a rogue operation." [redacted] Principal Deputy and Acting Assistant Attorney General Steven G. Bradbury told us that the DoJ certifications served as official confirmation that DoJ had determined that the activities carried out under the program were lawful.

~~(S//NF)~~ Gonzales told us that approval of the program as to form and legality was not required as a matter of law, but he believed that it "added value" to the Presidential Authorization for three reasons. First, NSA was being asked to do something it had not done before, and it was important to assure the NSA that the Attorney General had

approved the legality of the program [redacted] Third, for "purely political considerations," the Attorney General's approval of the program would have value "prospectively" in the event of Congressional or inspector general reviews of the program.

(U) The Presidential Authorizations were issued at intervals of approximately 30 to 60 days. Bradbury said that the main reason for periodically reauthorizing the program was to ensure that the Presidential Authorizations were reviewed frequently to assess the program's value and effectiveness. As the period for each Presidential Authorization drew to a close, the DCI prepared a threat assessment memorandum for the President describing the current state of potential terrorist threats to the United States.

(U) The Threat Assessment Memorandums Supporting Presidential Authorization of the Program

~~(S//NF)~~ From October 2001 to May 2003, the CIA prepared the threat assessment memorandums that supported Presidential authorization and periodic reauthorization of the PSP. The memorandums documented the current threat to the U.S. homeland and to U.S. interests abroad from al-Qa'ida and affiliated terrorist organizations. The first threat assessment memorandum—*The Continuing Near-Term Threat from Usama Bin Ladin*—was signed by the DCI on 4 October 2001.[7] Subsequent threat assessment memorandums were prepared every 30 to 60 days to correspond with the President's reauthorizations.

~~(S//NF)~~ The DCI Chief of Staff, John H. Moseman, was the CIA focal point for preparing the threat assessment memorandums. According to Moseman, he directed the CIA, [redacted] to prepare objective appraisals of the current terrorist threat, focusing primarily on threats to the homeland, and to document those appraisals in a memorandum. [redacted] analysts drew upon all sources of intelligence in preparing their threat assessments. Each of the memorandums focused primarily on the current threat situation and did not routinely provide information concerning previously reported threats or an assessment of the PSP's utility in addressing previously reported threats.

~~(S//NF)~~ After [redacted] completed its portion of the memorandums, Moseman added a paragraph at the end of the memorandums stating that the individuals and organizations involved in global terrorism (and discussed in the memorandums) possessed the capability and intention to undertake further terrorist attacks within the United States. Moseman recalled that the paragraph was provided to him initially by either Gonzales or Addington. The paragraph recommended that the President authorize the Secretary of Defense to employ within the United States the capabilities of DoD, including but not limited to NSA's SIGINT capabilities, to collect foreign intelligence by electronic surveillance. The paragraph described the types of communication and data that would be collected and the

[7] (U) The title of the threat assessment memorandums was changed to *The Global War Against Terrorism* in June 2002.

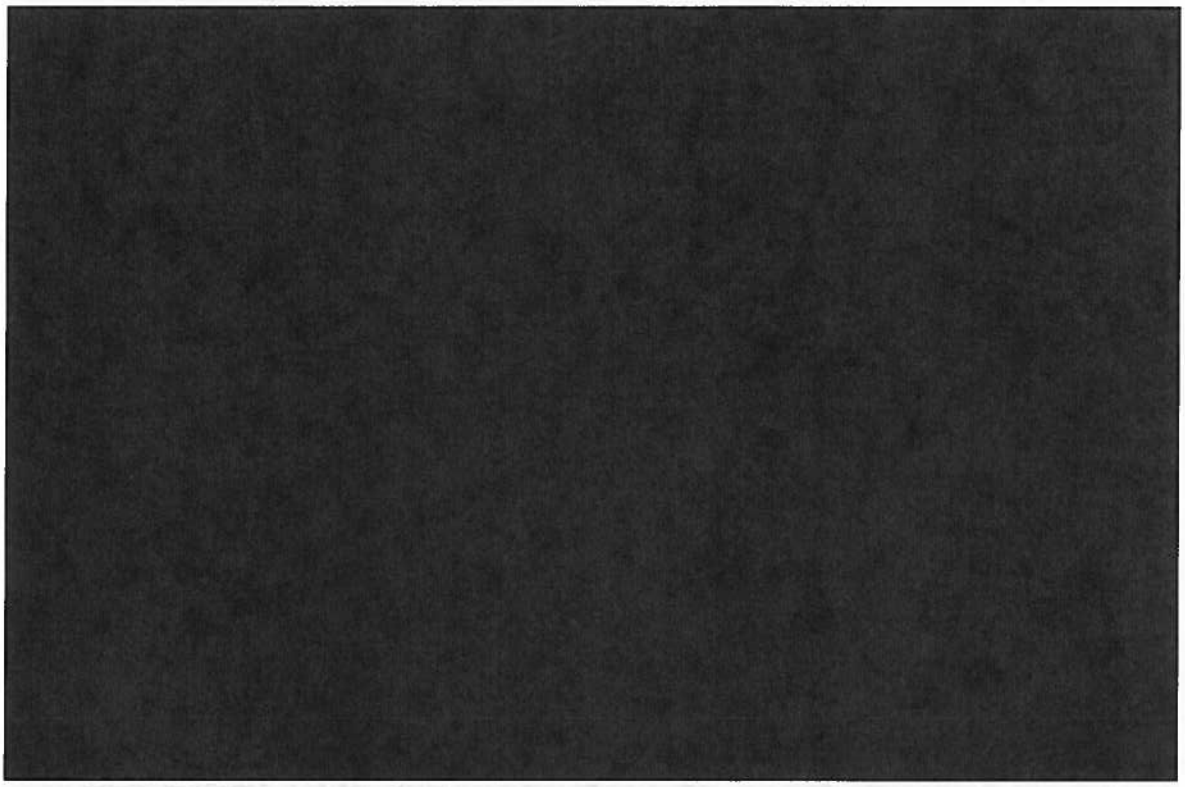
circumstances under which they could be collected. The draft threat assessment memorandums were reviewed by CIA Office of General Counsel attorneys assigned to [redacted] and CIA Acting General Counsel (Principal Deputy General Counsel), John A. Rizzo. Rizzo told us that the draft memorandums were generally sufficient, but there were occasions when, based on his experience with previous memorandums, he thought that draft memorandums contained insufficient threat information or did not present a compelling case for reauthorization of the PSP. In such instances, Rizzo would request that [redacted] provide additional available threat information or make revisions to the draft memorandums.

~~(S//NF)~~ The threat assessment memorandums were then signed by the DCI and forwarded to the Secretary of Defense to be co-signed. Tenet signed most of the threat memorandums prepared during his tenure as DCI. There were no occasions when the DCI or Acting DCI withheld their signature from the threat assessment memorandums. The threat assessment memorandums were reviewed by DoJ's OLC to assess whether there was "a sufficient factual basis demonstrating a threat of terrorist attacks in the United States for it to continue to be reasonable under the standards of the Fourth Amendment for the President to [continue] to authorize the warrantless searches involved" in the program. OLC then advised the Attorney General whether the constitutional standard of reasonableness had been met and whether the Presidential Authorization could be certified as to form and legality. After review and approval as to form and legality by the Attorney General, the threat assessment memorandums were delivered to the White House to be attached to the PSP reauthorization memorandums signed by the President.

~~(S//NF)~~ Responsibility for drafting the threat assessment memorandums was transferred from [redacted] to the newly-established Terrorist Threat Integration Center in May 2003. This responsibility was retained by TTIC's successor organization, NCTC. The DCI continued to sign the threat assessment memorandums through 15 April 2005. Subsequent memorandums were signed by the Director of National Intelligence or his designee.

(U) Early Revisions to the Presidential Authorizations

~~(TS//STLW//SI//OC/NF)~~ On 2 November 2001, with the first authorization set to expire, President Bush signed a second Presidential Authorization of the PSP. The second authorization cited the same authorities in support of the President's actions, principally the Article II Commander-in-Chief powers and the AUMF. The second authorization also cited the same findings of a threat assessment concerning the magnitude of potential terrorist threats and the likelihood of their occurrence in the future. [redacted]



~~(TS//STLW//SI//OC/NF)~~ On 30 November 2001, the President signed a third authorization for the PSP.

[redacted]

(U) DoJ Office of Legal Counsel Memorandums Supporting Legality of the Program

~~(S//NF)~~ OLC Deputy Assistant Attorney General John Yoo was responsible for drafting the first series of legal memorandums supporting the PSP. Yoo was the only OLC official read into the PSP from the program's inception until he left DoJ in May 2003.

During Yoo's tenure at DoJ, he was one of only three DoJ officials read into the PSP. The other two were Ashcroft and Baker. OLC Assistant Attorney General Jay S. Bybee, Yoo's direct supervisor, was never read into the program.

~~(S//NF)~~ Before the President authorized the PSP on 4 October 2001, Yoo had prepared a memorandum evaluating the legality of a hypothetical electronic surveillance program within the United States to monitor communications of potential terrorists. His memorandum, dated 17 September 2001, was addressed to Deputy White House Counsel Timothy E. Flanigan and was entitled *Constitutional Standards on Random Electronic Surveillance for Counter-Terrorism Purposes*. Yoo drafted a more extensive version of the memorandum, dated 4 October 2001, for Gonzales.

[redacted]

[redacted]

~~(S//NF)~~ The first OLC memorandum explicitly addressing the legality of PSP was not drafted until after the program had been formally authorized by the President and after Ashcroft had certified the program as to form and legality. The first OLC opinion directly supporting the legality of the PSP was dated 2 November 2001, and was drafted by Yoo. Yoo acknowledged at the outset of his 2 November memorandum that "[b]ecause of the highly sensitive nature of this subject and the time pressures involved, this memorandum has not undergone the usual editing and review process for opinions that issue from our Office [OLC]."

[redacted]

~~(S//NF)~~ Yoo acknowledged in his 2 November 2001 memorandum that the first Presidential Authorization was "in tension with FISA." Yoo stated that FISA "purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence." But Yoo then opined that "[s]uch a reading of FISA would be an unconstitutional infringement on the President's Article II authorities." Citing advice of OLC and DoJ's position as presented to Congress during passage of the USA PATRIOT Act several weeks earlier, Yoo characterized FISA as merely providing a "safe harbor for electronic surveillance," adding that it "cannot restrict the President's ability to engage in warrantless searches that protect the national security."

~~(S//NF)~~ Regarding whether the activities conducted under the PSP could be conducted under FISA, Yoo described the same potential impediments that he had cited in his 4 October memorandum. Noting that the Presidential Authorization could be viewed as a violation of FISA's civil and criminal sanctions in 50 U.S.C. §§ 1809-10, Yoo opined that in this regard FISA represented an unconstitutional infringement on the President's Article II powers. According to Yoo, the ultimate test of whether the government may engage in warrantless electronic surveillance activities is whether such conduct is consistent with the Fourth Amendment, not whether it meets the standards of FISA.

~~(S//NF)~~ Yoo wrote that reading FISA to restrict the President's inherent authority to conduct foreign intelligence surveillance would raise grave constitutional questions which, under the doctrine of constitutional avoidance, would require resolving the issue in a manner that preserves the President's [redacted] "[U]nless Congress made a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless searches in the national security area—which it has not—then the statute must be construed to avoid such a reading."

~~(TS//SI//NF)~~ Yoo's 2 November 2001 memorandum dismissed Fourth Amendment concerns to the extent that the authorized collection involved non-U.S. persons outside the United States. Regarding those aspects of the program that involved interception of the international communications of U.S. persons within the United States, Yoo asserted that Fourth Amendment jurisprudence allowed for searches of persons crossing U.S. international borders and that interceptions of communications into or out of the United States fell within the "border crossing exception." Yoo further opined that electronic surveillance in "direct support of military operations" did not trigger constitutional protection against illegal searches and seizures, in part because the Fourth Amendment is primarily aimed at curbing law enforcement abuses. Finally, Yoo wrote that the electronic surveillance described in the Presidential Authorizations was "reasonable" under the Fourth Amendment and therefore did not require a warrant, i.e., in this situation the government's national security interest outweighed the individual's privacy interest.

[redacted]

~~(TS//SI//NF)~~ In October 2002, at Ashcroft's request, Yoo drafted another opinion concerning the PSP. The memorandum, dated 11 October 2002, reiterated the same basic analysis as Yoo's 2 November 2001 memorandum in support of the legality of the PSP.

[redacted]

(U) IMPLEMENTATION OF THE PRESIDENT'S SURVEILLANCE PROGRAM

(U) NSA Implementation

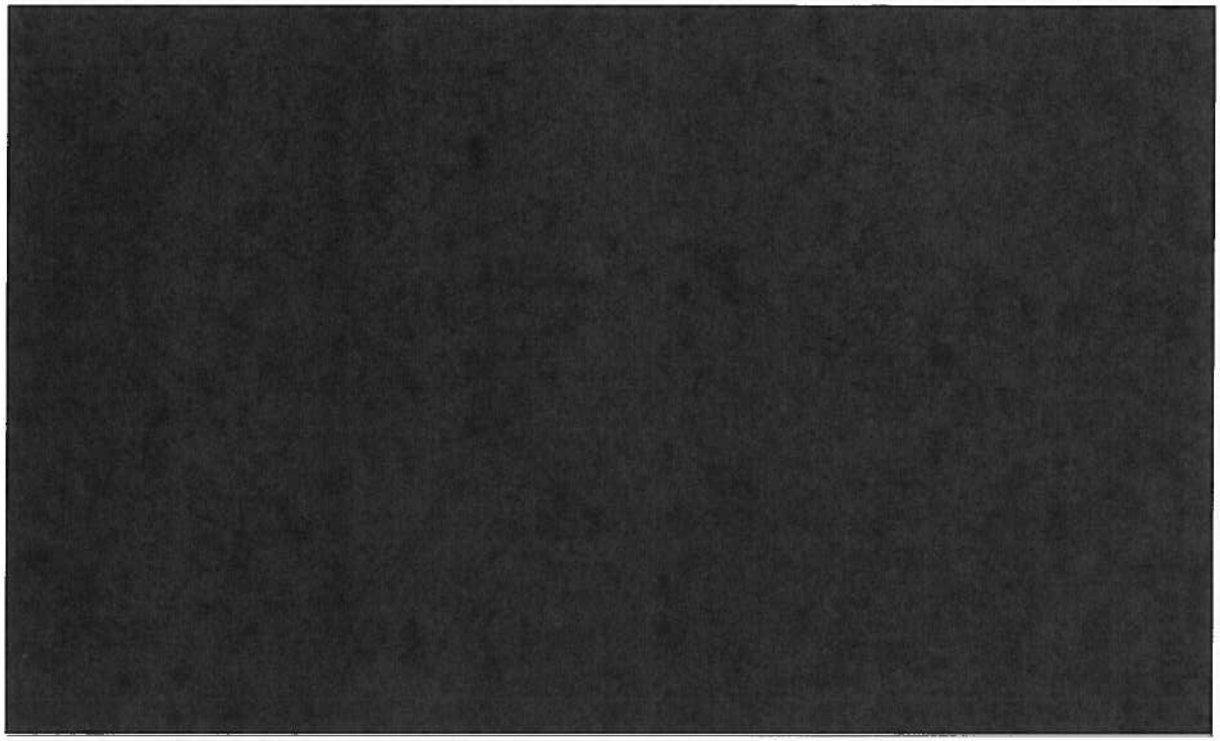
~~(S//NF)~~ On 4 October 2001, Hayden received the initial Presidential Authorization of the PSP and briefed the NSA SIGINT Director and other key NSA personnel on the authorization. [redacted] He also said that the NSA General Counsel had reviewed the authorization and concluded that the authorized activities were legal.

[redacted]

[redacted]

[redacted] NSA began to collect the content of telephone calls under PSP authority in October 2001.

[redacted]



~~(TS//SI//NF)~~ **Telephone and Internet Communications Content Collection and Analysis**

~~(TS//SI//NF)~~ Content collection and analysis under the PSP was conducted in the same manner as collection and analysis conducted previously by the NSA under E.O. 12333 authority. NSA management applied standard minimization and specially designed procedures to task domestic selectors such as telephone numbers and e-mail addresses. Selectors had to meet two criteria before being tasked under the PSP: the purpose of the collection had to be to prevent and detect terrorist attacks in the United States; and the selector had to be linked to al-Qa'ida, an associate, or international terrorism.

~~(TS//SI//NF)~~ NSA collection managers were responsible for ensuring that telephony and Internet communications selectors were appropriately added or removed from collection. Content collection for domestic selectors was sometimes approved for specific

time periods. Data collected under the PSP were stored in compartmented NSA databases, and access to the databases was strictly controlled.

~~(TS//SI//OC/NF)~~ The majority of targets for content collection under the PSP were foreign telephone numbers and Internet communications addresses. In 2008, NSA reported that [redacted] foreign telephone numbers and in excess of [redacted] foreign Internet communications addresses had been targeted from October 2001 through December 2006. NSA reported in 2008 tha[redacted] domestic telephone numbers and [redacted] domestic Internet communications addresses were targeted for PSP content collection from October 2001 to January 2007. Although targeted domestic telephone numbers and Internet communications addresses were located in the United States, they were not necessarily used by U.S. citizens.

[redacted]

~~(S//NF)~~ PSP program officials told us that the NSA did not seek to collect domestic communications under the PSP. However, NSA managers said that there are no readily available technical means within the [redacted] to guarantee that no domestic calls will be collected. Issues of this kind inevitably arise from time to time in other SIGINT operations, and are not unique to the PSP. Over the life of the program, the NSA reported [redacted] incidents of unintentional collection of domestic communications or non-targeted communications. In such cases, the NSA IG determined that personnel followed established procedures in reporting the incidents, adjusting collection, and purging unauthorized collection records from NSA databases.

~~(TS//SI//NF)~~ NSA analysis of content collected under the PSP involved the same practices and techniques used in analyzing information from other SIGINT operations. Telephone content was made available to NSA analysts through a voice processing system; Internet communications content was available from the database in which it was stored. Analysis involved more than listening to, or reading the content of, a communication and transcribing and disseminating a transcript. Analysis also involved coordinating and collaborating with other IC analysts, applying previous knowledge of the target, and integrating other relevant intelligence.

~~(TS//SI//NF)~~ Telephony and Internet Metadata Collection and Analysis

~~(TS//SI//OC/NF)~~ [redacted] NSA personnel used PSP metadata to perform contact chaining. Although the NSA had the capability to collect bulk telephony and Internet metadata before the PSP, collection was limited because the NSA was not authorized to collect metadata from a wire inside the United States without a court order when one end of the communication was in the United States. NSA could "chain" to, but not through, domestic selectors. Access to large amounts of metadata is required for effective contact chaining, and the PSP increased the data available to NSA analysts and allowed them to perform more thorough contact chaining.

~~(TS//SI//OC/NF)~~ Although NSA analysts could search bulk-collected metadata under the PSP, the analysts' searches were limited to targets that were approved under the standards set forth in the Presidential Authorizations. As such, only a small fraction of the metadata collected under the PSP was ever accessed. In August 2006, the NSA estimated that 0.000025 percent of the telephone records in the PSP database (or one of every four million records) could be expected to be seen by NSA analysts through chaining analysis.

[redacted]

~~(TS//SI//NF)~~ NSA analysts conduct contact chaining by entering a target selector—a telephone number or Internet communication address—in a specialized metadata analysis tool, which searches the metadata and identifies contacts between the selector and other telephone numbers or Internet communications addresses. The resulting contact graph is analyzed for intelligence and to develop investigative leads. [redacted] Although the Presidential Authorizations did not prohibit chaining more than two degrees of separation from the target, NSA analysts determined that it was not analytically useful to do so.

~~(TS//SI//NF)~~ An automated process was created to alert and automatically chain new and potentially reportable telephone numbers using what was called an "alert list." Telephone numbers on the alert list were automatically run against incoming metadata to look for contacts. [redacted]

[redacted]

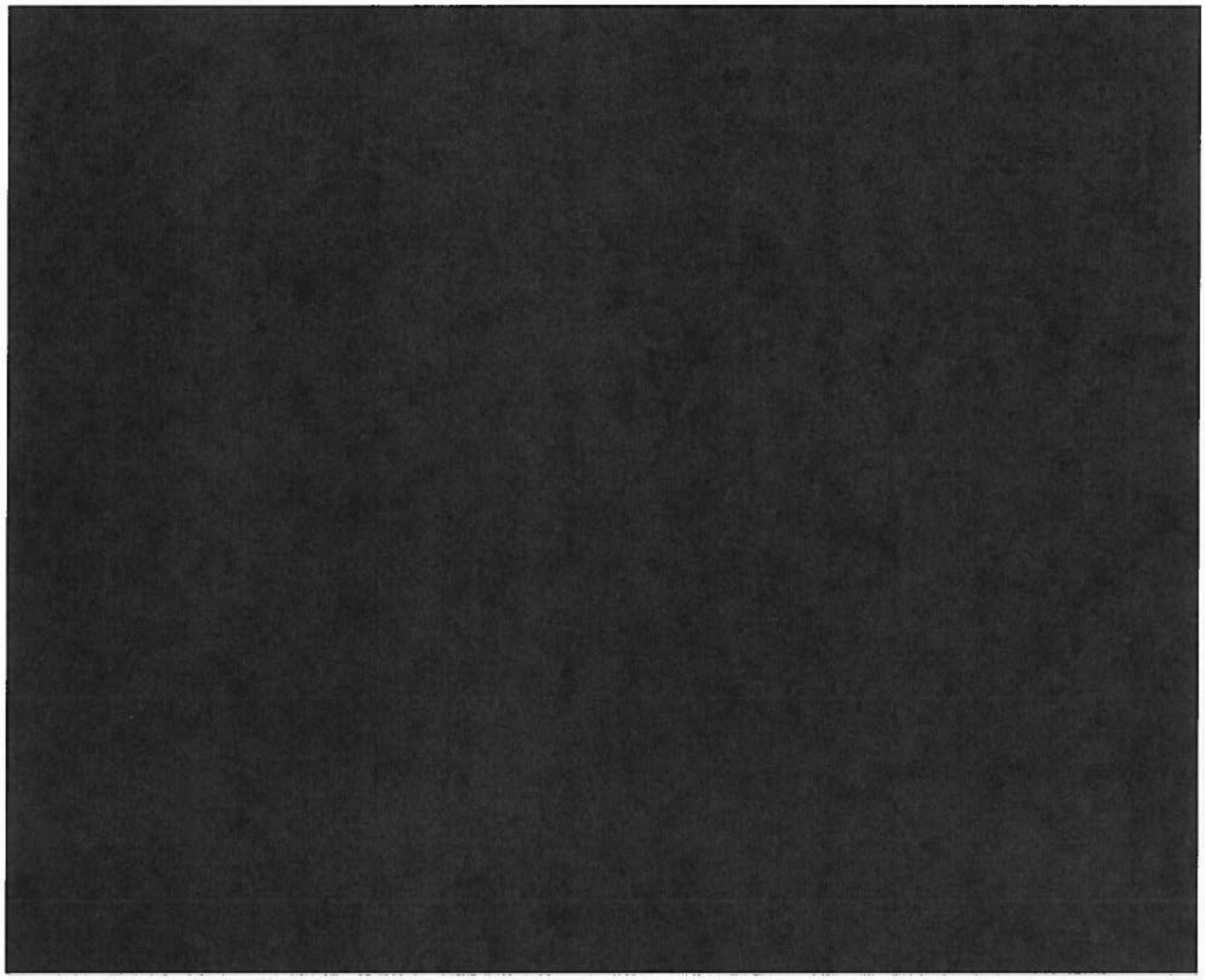
~~(TS//SI//NF)~~ When NSA personnel identified erroneous metadata collection—usually caused by technical problems or inappropriate application of the authorization—they were directed to report the violation or incident through appropriate channels and to delete the collection from all NSA databases. NSA reported three such violations early in the program and took measures to correct them.

(U) NSA Reporting From the President's Surveillance Program

~~(TS//SI//OC/NF)~~ PSP information was disseminated in [redacted] types of reports: "tippers," which provided metadata analysis; content reports, which provided NSA analysis of content collection; [redacted] Tippers were sent to the FBI and the CIA by e-mail on a secure communications network. Some tippers contained "tear line" information that allowed for wider distribution of a sanitized version of the information. From October 2001 through January 2007, the NSA issued [redacted] tippers to the FBI and the CIA.[8]

[redacted]

[redacted]



(U) NSA Managerial Structure and Oversight of the President's Surveillance Program

~~(S//NF)~~ Analysis and reporting associated with the PSP was conducted within SID at NSA's Fort Meade, Maryland headquarters. PSP activities were not conducted at NSA field sites. The Director and Deputy Director of NSA exercised senior operational control and authority over the program. The individual who was SIGINT Director in 2001 told us that, aside from ensuring that the PSP had appropriate checks and balances, she left direct management of the program to the NSA Director, the Deputy Director, and the Office of General Counsel. She noted that Hayden took personal responsibility for the program and managed it carefully.

~~(S//NF)~~ By 2004, specific managerial authorities concerning PSP collection, analysis, and reporting activities had been delegated to the SIGINT Director. The SIGINT Director further delegated managerial authority to the PSP program manager and mission execution responsibilities to the Chief of the CT Product Line. The PSP program manager position was restructured to provide the incumbent authority and responsibility for oversight of PSP

activity across SID, and the PSP program manager was provided additional staff. Over the life of the program, there were five PSP program managers, who reported directly to the SIGINT Director or the Chief of the CT Product Line.

~~(TS//STLW//SI//OC/NF)~~ The NSA supported the operation of the PSP with approximately [redacted] from fiscal years (FYs) 2002 through 2006. Funds were used for the acquisition of [redacted]

(U) NSA PSP Costs From FY 2002 through FY 2006
(dollars in thousands, personnel costs not included)

~~(TS//STLW//SI//OC/NF)~~

[redacted]

(U) NSA Management Controls to Ensure Compliance With Presidential Authorizations

~~(S//NF)~~ NSA management took steps to protect U.S. person information and ensure compliance with the Presidential Authorizations. [redacted]

[redacted]

~~(S//NF)~~ The NSA General Counsel was read into the PSP on 4 October 2001, the day the first Presidential Authorization was signed. On 6 October 2001, the General Counsel provided Hayden and his deputy talking points for use in briefing NSA personnel on the new program's authorities. The talking points included the fact that Hayden had directed the NSA General Counsel and the NSA Associate General Counsel for Operations to review and oversee PSP activities. The NSA Associate General Counsel for Operations provided most of the program oversight before the NSA IG was read into the PSP in August 2002. The Associate General Counsel for Operations oversaw program implementation, reviewed proposed target packages for compliance with the authorizations, and coordinated program-related issues with DoJ.

(U) NSA Inspector General Oversight of the Program

~~(S//NF)~~ The NSA IG and other NSA Office of Inspector General personnel were read into the PSP beginning in August 2002. Over the life of the program, the NSA IG conducted:

- Three investigations in response to specific incidents and violations of the Presidential Authorizations to determine the cause, effect, and remedy.
- Ten reviews to determine the adequacy of management controls to ensure compliance with the authorization and related authorities, assess the mitigation of risk associated with program activities, and identify impediments to meeting the requirements of the authorizations.

~~(TS//SI//NF)~~ Ten of the NSA IG reports included a total of [redacted] recommendations to NSA management to strengthen internal controls and procedures over the PSP. The NSA IG identified no intentional misuse of the PSP. Significant findings from NSA IG reviews of the PSP include the following:

- In 2005, the NSA IG found [redacted] errors when comparing records of domestic telephone and communications selectors approved for PSP content collection with selectors actually on collection. The errors included selectors that were not removed from collection after being detasked, selectors that were not put on collection when approved, and selectors that were mistakenly put on collection due to typographical errors. NSA management took steps to correct the errors and establish procedures to reconcile approved selectors with selectors actually on collection.
- During a 2006 review, the NSA IG found that all items in a randomly selected sample of domestic selectors met Presidential Authorization criteria. Using a statistically valid sampling methodology, the IG concluded with 95 percent confidence that 95 percent or more of domestic

selectors tasked for PSP content collection were linked to al-Qa'ida, its associates, or international terrorist threats inside the United States.

~~(S//NF)~~ In addition to NSA IG report recommendations, in March 2003, the NSA IG recommended to Hayden that he report violations of the Presidential Authorizations to the President. The NSA IG prepared [redacted] Presidential notifications for the NSA Director concerning violations of the authorizations.

~~(S//NF)~~ Beginning in January 2007, violations involving collection activities conducted under PSP authority as well as violations related to former PSP activities that were operating under FISA authority were reported quarterly to the President's Intelligence Oversight Board, through the Assistant to the Secretary of Defense for Intelligence Oversight.

~~(TS//SI//NF)~~ The NSA IG learned in late 2008, that from approximately [redacted] collection of [redacted] All related collection records were purged from NSA databases in 2004; therefore, it was not possible to determine the exact nature and extent of the collection. NSA OIG will close out this incident in its upcoming report to the President's Intelligence Oversight Board.

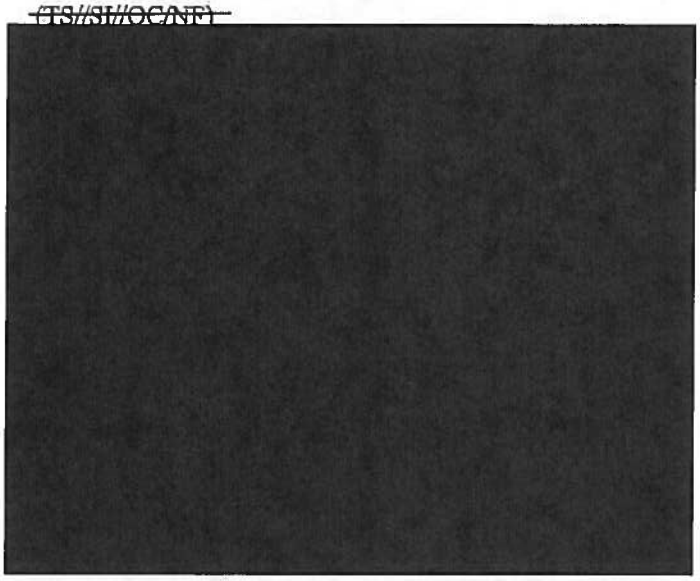
~~(TS//SI//NF)~~ On 15 January 2009, the DoJ reported to the FISC that the NSA had been using an "alert list" to compare FISA-authorized metadata against telephone numbers associated with counterterrorism targets tasked by the NSA for SIGINT collection. The NSA had reported to the FISC that the alert list consisted of telephone numbers for which NSA had determined the existence of a reasonable, articulable suspicion that the numbers were related to a terrorist organization associated with [redacted] In fact, such a determination had not been made for the majority of the selectors on the alert list. The NSA IG reported this incident to the President's Intelligence Oversight Board, and has provided updates as required. The alert list and a detailed NSA 60-day review of processes related to the business records FISC order were the subject of several recent submissions to the FISC and of NSA briefings to the Congressional oversight committees.

(U) Access to the President's Surveillance Program

[redacted]

(U) PSP Cumulative Clearance Totals
(as of 17 January 2007)

~~(TS//SI//OC/NF)~~



~~(S//NF)~~ Knowledge of the PSP was strictly controlled and limited at the express direction of the White House. Hayden eventually delegated his PSP clearance approval authority for NSA, FBI, and CIA operational personnel to the NSA PSP program manager. Hayden was required to obtain approval from the White House to clear members of Congress, FISC Judges, the NSA IG, and others.

~~(S//NF)~~ The NSA IG was not read into the PSP until August 2002. According to the NSA General Counsel at the time, the President would not allow the IG to be briefed prior to that date. Although Hayden did not recall why the IG had not been cleared earlier, he thought that it would have been inappropriate to clear him when the length of the program was unknown and before operations had stabilized. By August 2002, Hayden and the NSA General Counsel wanted to institutionalize PSP oversight with the involvement of the NSA IG. Hayden recalled having to "make a case" to the White House to have the NSA IG read in. The ODNI IG found that ODNI oversight of the PSP was limited by ODNI oversight personnel not being provided timely access to the program.

(U) Congressional Briefings on the Program

~~(TS//SI//NF)~~ On 25 October 2001, Hayden conducted a briefing on the PSP for the Chairman and the Ranking Member of the House Permanent Select Committee on Intelligence, Nancy P. Pelosi and Porter J. Goss; and the Chairman and the Vice Chairman of the Senate Select Committee on Intelligence (SSCI), D. Robert Graham and Richard C. Shelby. Between 25 October 2001 and 17 January 2007, Hayden and current NSA Director Alexander, sometimes supported by other NSA personnel, conducted

49 briefings to members of Congress and their staff. Hayden told us that during the many PSP briefings to members of Congress, no one ever suggested that the NSA should stop the program. Hayden emphasized that he did more than just "flip through slides" during the briefings, which lasted as long as attendees had questions.

(U) Foreign Intelligence Surveillance Court Briefings on the Program

~~(TS//SI//OC/NF)~~ On 31 January 2002, the FISC Presiding Judge Royce Lamberth became the first member of the court to be read into the PSP. He was briefed on the program after James Baker, the head of DoJ's Office of Intelligence Policy and Review (OIPR) [redacted] Lamberth's briefing was conducted at the DoJ and was attended by Ashcroft, Hayden, Mueller, Yoo, and Baker.

~~(TS//SI//OC/NF)~~ Ashcroft provided Lamberth a brief summary of the President's decision to create the PSP, and Ashcroft stated that he had determined, based upon the advice of John Yoo, an attorney in DoJ's Office of Legal Counsel (OLC), that the President's actions were lawful under the Constitution. Ashcroft also emphasized to Lamberth that the FISC was not being asked to approve the program. Following Ashcroft's summary, Hayden described for Lamberth how the program functioned operationally, Yoo discussed legal aspects of the program, and Baker proposed procedures for handling international terrorism FISA applications that contained PSP-derived information. For the next four months, until the end of his term in May 2002, Lamberth was the only FISC judge read into the PSP.

~~(TS//SI//OC/NF)~~ Judge Colleen Kollar-Kotelly succeeded Lamberth as the FISC Presiding Judge and was briefed on the PSP on 17 May 2002. The briefing was similar in form and substance to that provided to Lamberth. In response to several questions from Kollar-Kotelly about the scope of the President's authority to conduct warrantless surveillance, DoJ prepared a letter to Kollar-Kotelly, signed by Yoo, that, according to Kollar-Kotelly, "set out a broad overview of the legal authority for conducting [the PSP], but did not analyze the specifics of the [PSP] program." The letter, which Kollar-Kotelly reviewed at the White House but was not permitted to retain, essentially replicated Yoo's 2 November 2001 memorandum regarding the legality of the PSP. Kollar-Kotelly was the only sitting FISC judge read into the PSP until January 2006, when the other FISC judges were read in.

~~(TS//SI//OC/NF)~~ Baker was read into the PSP only after he came upon "strange, unattributed" language in a FISA application that suggested the existence of a compartmented program. [redacted] As noted, eventually Lamberth, and later his successor, Kollar-Kotelly, were read in. The DoJ IG believes that not having OIPR officials and members of the FISC read into the PSP, while program-derived information was being disseminated as investigative leads to the FBI and finding its way into FISA

applications, put at risk the DoJ's important relationship with the FISC. The DoJ IG agrees with Baker's assessment that, as the government's representative before the FISC, good relations between the DoJ and the FISC depend on candor and transparency.

(U) FBI Participation in the President's Surveillance Program

~~(TS//SI//NF)~~ As a user of PSP-derived information, the FBI disseminated leads—tippers—to FBI field offices. Tippers primarily consisted of domestic telephone numbers and Internet communications addresses that NSA analysts had determined through metadata analysis were connected to individuals involved with al-Qa'ida or its affiliates. Domestic telephone numbers represented the overwhelming majority of PSP-derived information contained in tippers. Tippers also provided information derived from content collection under the PSP.

~~(TS//SI//NF)~~ The FBI's principal objective during the earliest months of the PSP was to disseminate program information to FBI field offices for investigation while protecting the source of the information and the methods used to collect it. The FBI initially assigned responsibility for this to its Telephone Analysis Unit (TAU), which developed procedures to disseminate information from NSA's PSP reports in a non-compartmented, Secret-level format. The resulting [redacted] Electronic Communications (ECs) included restrictions on how the information could be used, i.e., FBI field offices were to use the information "for lead purposes only" and not use the information in legal or judicial proceedings.

~~(S//NF)~~ The FBI's participation in the PSP evolved over time as the program became less a temporary response to the September 11 attacks and more a permanent surveillance capability. To improve the effectiveness of its participation in the program, the FBI initiated the [redacted] project in [redacted] to manage its involvement in the PSP. In February 2003, the FBI assigned a team of FBI personnel—"Team 10"—to work full-time at the NSA to manage the FBI's participation in the program.

(TS//SI//NF) Team 10's primary responsibility was to disseminate PSP information through [redacted] ECs to FBI field offices for investigation or other purposes. However, over time, Team 10 began to participate in the PSP in other ways. For example, Team 10 occasionally submitted telephone numbers and Internet communications addresses to the NSA to be searched against the bulk metadata collected under the PSP. The NSA conducted independent analysis to determine whether telephone numbers or Internet communications addresses submitted by Team 10 met the standards established by the Presidential Authorizations. Team 10 also regularly contributed to NSA's PSP process by reviewing draft reports and providing relevant information from FBI databases.

~~(S//NF)~~ FBI field offices were not required to investigate every tipper disseminated by Team 10 under the [redacted] project. Rather, the type of lead that the [redacted] EC assigned—"action," "discretionary," or "for information"—drove the field office's

response to a tipper.[9] The vast majority of FBI investigative activity related to PSP information involved responding to [redacted] telephone number tippers that assigned action leads. Team 10 generally assigned action leads for telephone numbers that were not already known to the FBI or telephone numbers that Team 10 otherwise deemed a high priority, such as a number that had a relationship to a major FBI investigation. From approximately [redacted] when [redacted] was established, to [redacted] action leads instructed field offices to obtain subscriber information for the telephone numbers within its jurisdiction and to conduct any "logical investigation to determine terrorist connections." Some agents complained that action leads lacked guidance about how to make use of the tippers, which was of particular concern because agents were not confident that [redacted] communications provided sufficient predication to open national security investigations.

~~(TS//SI//NF)~~ Two changes to FBI procedures in 2003 addressed some FBI agents' concerns. [redacted] FBI Headquarters assumed responsibility from field offices for issuing national security letters (NSLs) to obtain subscriber information about PSP-tipped telephone numbers and Internet communications addresses. [redacted] the Attorney General issued new guidelines for FBI national security investigations that created a new category of investigative activity called a "threat assessment." Under a threat assessment, FBI agents are authorized to investigate or collect information on individuals, groups, and organizations of possible investigative interest without opening a preliminary or full national security investigation. Beginning [redacted] action leads assigned by [redacted] metadata tippers instructed field offices to conduct threat assessments and advised that FBI headquarters would issue NSLs to obtain subscriber information.

~~(S//NF)~~ In general, an FBI threat assessment involved searching several FBI, public, and commercial databases for information about the tipped telephone number, and requesting that various state and local government entities conduct similar searches. Sometimes these searches identified the subscriber to the telephone number before FBI Headquarters obtained the information with an NSL. In other cases, the threat assessments continued after the field office received the NSL results.

~~(S//NF)~~ The [redacted] leads frequently were closed after conducting a threat assessment interview with the subscriber and determining that there was no nexus to terrorism or threat to national security. In other cases, the leads were closed based solely on the results of database checks.

~~(S//NF)~~ Beginning [redacted] FBI field offices were required to report the results of their threat assessments to FBI headquarters. FBI field offices typically reported all of the information that was obtained about the tipped telephone numbers, including the details of any subscriber interviews, and then stated that the office had determined that the

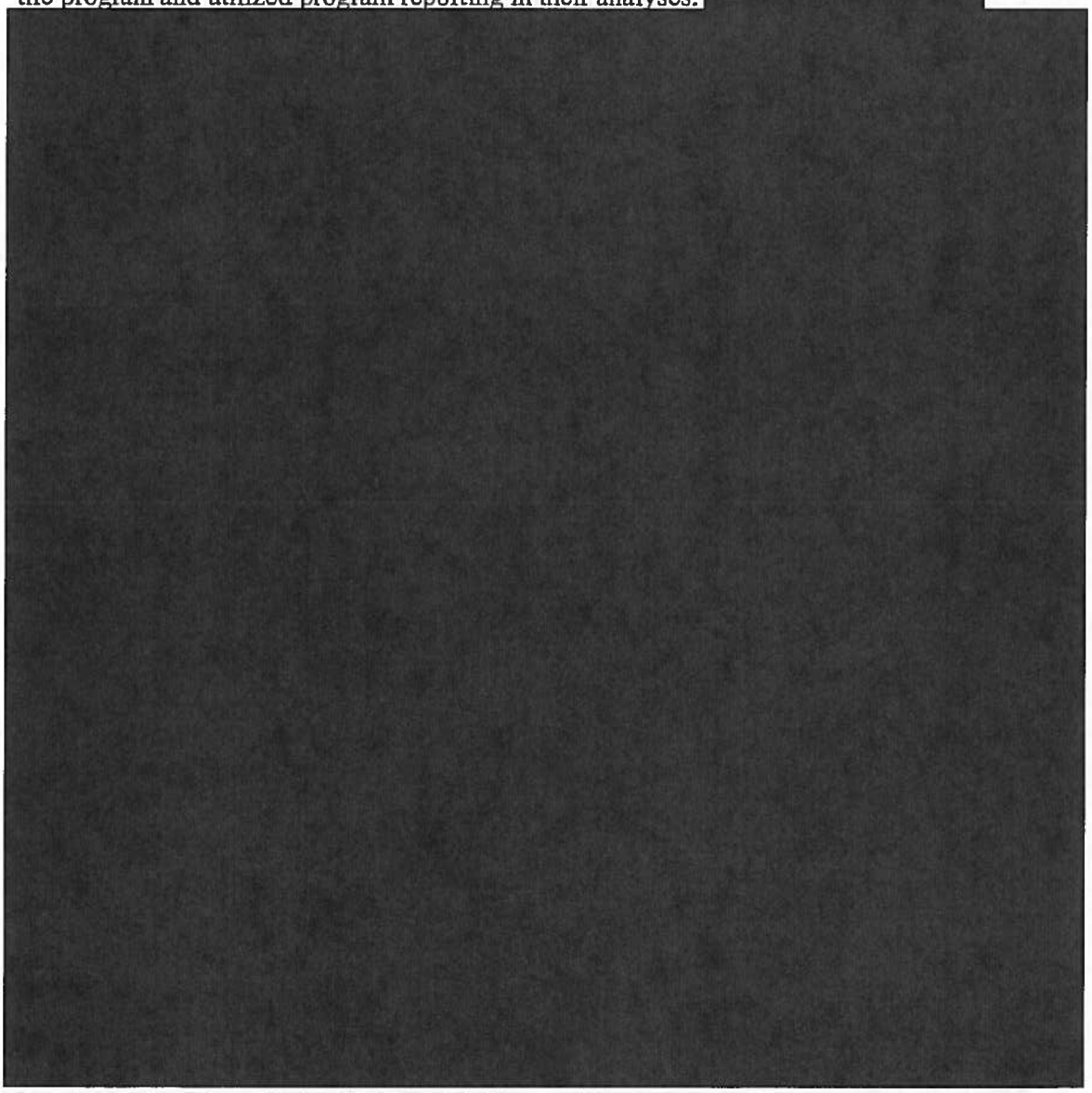
---

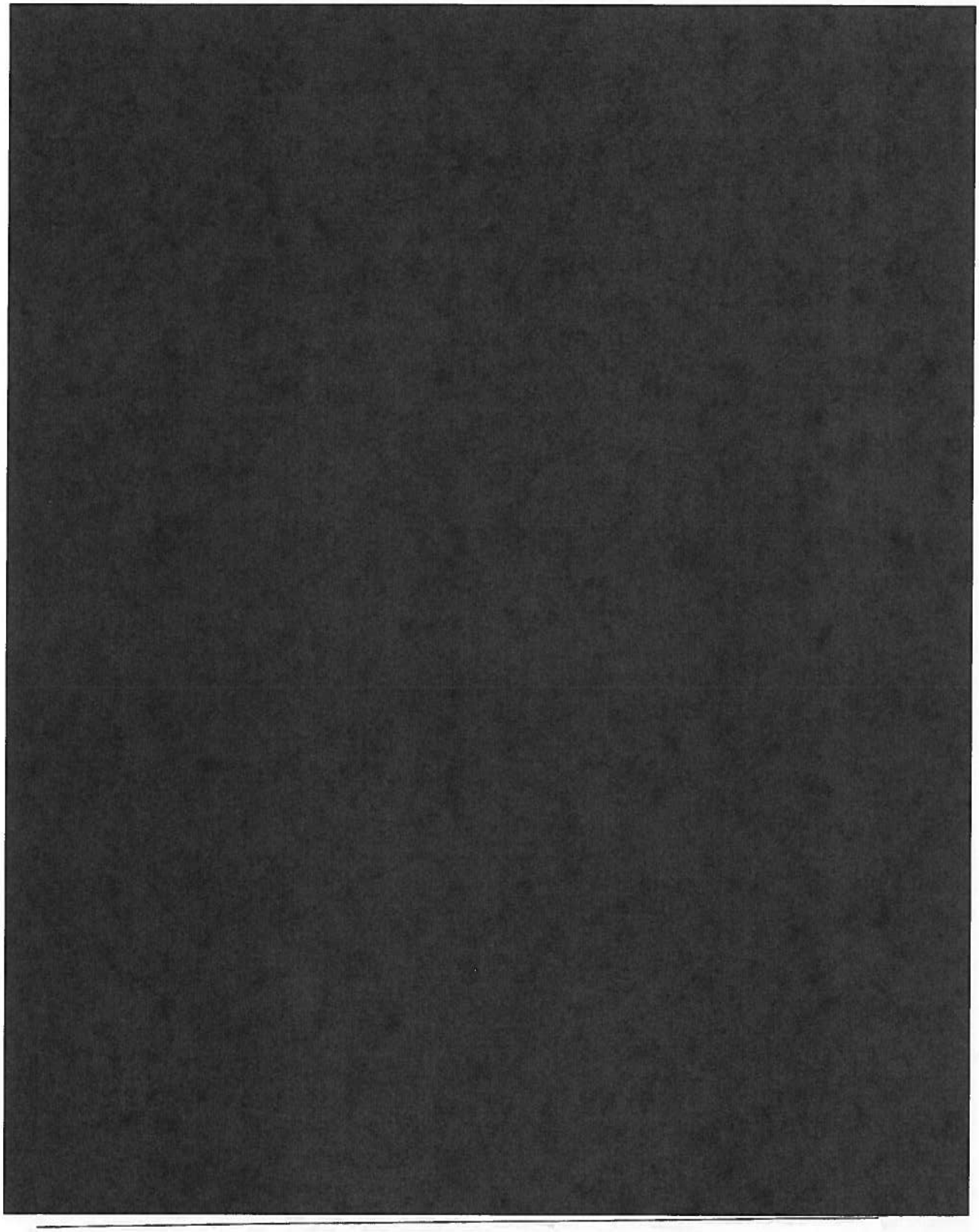
[9] ~~(S//NF)~~ An action lead instructs an FBI field office to take a particular action in response. A discretionary lead allows the field office to make a determination whether the information provided warrants investigative action. A field office is not expected to take any specific action on a for information lead.

telephone number did not have a nexus to terrorism and considered the lead closed. Much less frequently, field offices reported that a preliminary investigation was opened. Regardless of whether any links to international terrorism were identified in a threat assessment, the results of the threat assessments and the information that was collected about subscribers generally were reported to FBI headquarters and uploaded to FBI databases.

(U) CIA Participation in the President's Surveillance Program

~~(S//NF)~~ CIA analysts and targeters, as PSP consumers, requested information from the program and utilized program reporting in their analyses.





[redacted]

(U) NCTC Participation in the President's Surveillance Program

~~(TS//SI//NF)~~ The ODNI IG found that the ODNI's primary role in the PSP was the preparation of the threat assessments that summarized the al-Qa'ida threat to the United States and were used to support periodic reauthorization of the program. The ODNI IG found that the threat assessments were drafted by experienced NCTC personnel who prepared the documents in a memorandum style following an established DoJ format. The ODNI IG also determined that the ODNI threat assessments were prepared using evaluated intelligence information chosen from a wide variety of IC sources. ODNI personnel said that during the period when the ODNI prepared the threat assessments, the IC had access to fully evaluated intelligence that readily supported an assessment that al-Qa'ida remained a significant threat to the United States.

~~(TS//SI//NF)~~ [redacted] The NCTC analysts told us that PSP information was subject to stringent security protections [redacted]

~~(S//NF)~~ The NCTC analysts said that they handle NSA surveillance information, including PSP information, consistent with the standard rules and procedures for handling NSA intelligence information including minimization of U.S. person identities. On those occasions when the NCTC analysts knew that a particular NSA intelligence product was derived from the PSP, the analysts told us they reviewed program information in the same manner as other incoming NSA intelligence products. If appropriate, NCTC analysts then incorporated the PSP information into analytical products being prepared for the Director of National Intelligence (DNI) and other senior intelligence officials. They identified the President's Terrorism Threat Report and the Senior Executive Terrorism Report as examples of the types of finished intelligence products that would, at times, contain PSP information.

(U) The President's Surveillance Program and the Foreign Intelligence Surveillance Court

~~(TS//SI//NF)~~ DoJ, initially with the FISC's concurrence and later at the court's direction, developed and implemented procedures—referred to as "scrubbing" procedures—to account for and make the court aware of instances when PSP-derived information was included in FISA applications. Lamberth required that all FISA applications that contained PSP-derived information, or that would result in simultaneous collection against particular targets under both the PSP and a FISC order, be filed with him only. Baker told us that Lamberth wanted to be informed of applications that contained PSP information and of dual coverage situations. According to Baker, the scrubbing procedures were a means of meeting his ethical duty of candor to the FISC without disclosing the existence of the PSP to uncleared judges.

~~(TS//SI//NF)~~ DoJ effectuated the scrubbing procedures by compiling lists of information contained in initial and renewal FISA applications that was attributed to the NSA and of all facilities targeted for electronic surveillance in the applications. These lists were sent to the NSA to determine whether any of the NSA-attributed information was PSP-derived and whether any of the facilities also were targeted under the PSP. The NSA communicated the results back to DoJ, which then filed the applications with the FISC consistent with the scrubbing procedures.

~~(TS//SI//NF)~~ Kollar-Kotelly continued the procedures that had been developed by Baker and agreed to by Lamberth for handling FISA applications that contained PSP-derived information. However, Kollar-Kotelly required DoJ to excise from FISA applications any information obtained or derived from the PSP. But Kollar-Kotelly also instructed Baker to alert her to any instances where an application's basis for the requisite probable cause showing under FISA was weakened by excising PSP information. In such cases, Kollar-Kotelly would then assess the application with the knowledge that additional relevant information had been excised.

~~(TS//SI//OC/NF)~~ Kollar-Kotelly also instructed DoJ to discontinue the practice employed under Lamberth of including in applications a descriptive phrase associated with [redacted] as a means of indicating that facilities targeted by the applications were also targeted under the PSP. Baker told us that while Kollar-Kotelly understood that instances of dual coverage would occur, she did not want to appear to judicially sanction PSP coverage.

~~(TS//SI//NF)~~ In March 2004, Kollar-Kotelly was informed of operational changes made to the PSP following a dispute between DoJ and the White House about the legal basis for certain aspects of the program. Kollar-Kotelly responded by imposing an additional scrubbing requirement to further ensure, to the extent possible, that PSP-derived information was not included in FISA applications. The FBI, in coordination with DoJ and NSA, was to determine whether a facility included in a FISA application—not just a targeted telephone number or Internet communication address—also appeared in a PSP report. Kollar-Kotelly permitted any such facility to remain in the application if it could be

demonstrated that the FBI had developed, independent of the PSP, an investigative interest in the facility, or that the FBI inevitably would have identified the facility in question through normal investigative steps. An OIPR official who was responsible for discussing such cases with Kollar-Kotelly told us that the judge generally accepted DoJ's assessment that there was a non-PSP investigative basis for a facility in question, or that the facility inevitably would have been discovered even in the absence of PSP-derived leads to the FBI.

~~(S//NF)~~ Implementing the scrubbing procedures, both under Lamberth and Kollar-Kotelly, was a complicated and time-consuming endeavor for OIPR staff. Baker, who until March 2004 was the only individual in OIPR read into the PSP, found himself having to ask OIPR attorneys to compile information about their cases, and sometimes to make changes to their FISA applications, without being able to provide an explanation other than that he had spoken to the Attorney General and the FISC about the situation. Baker regularly told attorneys that they did not have to sign applications that they were not comfortable with, and, in some instances, international terrorism cases had to be reassigned for this reason.

~~(S//NF)~~ The situation was further complicated by the fact that, until August 2003, only one of the two DoJ officials authorized by statute to approve FISA applications—Attorney General Ashcroft and Deputy Attorney General Larry Thompson—was read into the PSP. Thompson, who served as Deputy Attorney General from May 2001 to August 2003, was never read into the PSP, despite Ashcroft's request to the White House.

~~(TS//SI//NF)~~ Similarly, Kollar-Kotelly, who by November 2004 was handling approximately [redacted] percent of all FISA applications as a result of her requirement that scrubbed applications be filed with her only, made unsuccessful requests for additional FISC judges to be cleared for the program. Kollar-Kotelly decided in November 2004 that in view of the scrubbing procedures that were in operation, international terrorism FISA applications could be decided by other judges based on the information contained in the applications.

~~(TS//SI//NF)~~ DoJ, together with the FBI and the NSA, continue to apply the scrubbing procedures to international terrorism FISA applications. Since January 2006, all members of the FISC have been briefed on the PSP and all of the judges handle applications that involve the issue of PSP-derived information. Although compliance with the scrubbing procedures has been burdensome, we did not find instances when the government was unable to obtain FISA surveillance coverage on a target because of the requirement. However, the DoJ IG concluded that once the PSP began to affect the functioning of the FISA process, OIPR and the FISC effectively became part of the PSP's operations, and more OIPR staff and FISC judges should have been read into the PSP to address the impact. Instead, access to the PSP was limited for years to a single OIPR official and one FISC judge.

(U) Discovery Issues Associated With the President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ DoJ was aware as early as [redacted] that information collected under the PSP could have implications for DoJ's litigation responsibilities under Rule 16 of the Federal Rules of Criminal Procedure and *Brady v. Maryland*, 373 U.S. 83 (1963). Analysis of the discovery issue was first assigned to Yoo in [redacted]

~~(S//NF)~~ No DoJ attorneys with terrorism prosecution responsibilities were read into the PSP until mid-2004, and as a result, DoJ did not have access to the advice of attorneys who were best equipped to identify and examine discovery issues associated with the PSP. The DoJ IG believes that, since then, DoJ has taken steps to respond [redacted] to [redacted] discovery motions [redacted] DoJ's responses to the discovery motions involve the use of the Classified Information Procedures Act, 18 U.S.C. App. 3, to file *ex parte* in camera pleadings with federal courts to describe potentially responsive PSP-derived information. [redacted]

~~(S//NF)~~ [redacted] the DoJ IG recommends that DoJ assess its discovery obligations regarding PSP-derived information in international terrorism prosecutions, carefully consider whether it must re-examine past cases to see whether potentially discoverable but undisclosed Rule 16 or *Brady* material was collected by the NSA, and take appropriate steps to ensure that it has complied with its discovery obligations in such cases. The DoJ IG also recommends that DoJ, in coordination with the NSA, implement a procedure to identify PSP-derived information that may be associated with international terrorism cases

currently pending or likely to be brought in the future and evaluate whether such information should be disclosed in light of the government's discovery obligations under Rule 16 and *Brady*.

(U) LEGAL REASSESSMENT OF THE PRESIDENT'S SURVEILLANCE PROGRAM (2003 – 2004)

~~(TS//SI//NF)~~ Concern Over the [redacted] Collection

~~(TS//SI//NF)~~ Yoo was the sole OLC attorney who advised Ashcroft and White House officials on the PSP from the program's inception in October 2001 through Yoo's resignation from DoJ in May 2003. Upon Yoo's departure, Patrick Philbin was selected by the White House to be read into the PSP to assume Yoo's role as advisor to the Attorney General concerning the program.

~~(TS//SI//NF)~~ Philbin told us that when he reviewed Yoo's legal memorandums about the PSP, he realized that Yoo had omitted from his analysis any reference to the FISA provision allowing the interception of electronic communications without a warrant for a period of 15 days following a Congressional declaration of war. (See 50 U.S.C. § 1811.) Philbin stated that Yoo's OLC opinions were premised on the assumption that FISA did not expressly apply to wartime operations, an assumption that from Philbin's perspective made the opinions "problematic."

[redacted]

[redacted]

~~(S//NF)~~ In August 2003, Philbin told Ashcroft that there were problems with the legal analysis supporting the PSP but probably not with the conclusions reached, and he therefore advised Ashcroft to continue to certify the program "as to form and legality." Philbin also recommended that a new OLC memorandum assessing the legality of the PSP be drafted, and with Ashcroft's concurrence he began drafting the memorandum.

(U) A New Legal Basis for the Program Is Adopted

~~(S//NF)~~ Goldsmith was sworn in as the Assistant Attorney General for OLC on 6 October 2003, replacing Bybee, who had left that position several months earlier to serve as a judge on the U.S. Court of Appeals for the Ninth Circuit. Philbin told us that he pressed hard to have Goldsmith read into the PSP, and that Addington told Philbin he would have to justify the request before Addington would take it to the President for a decision. Addington subsequently read Goldsmith into the program on 17 November 2003.

~~(TS//SI//NF)~~ After reviewing Yoo's memorandums and Philbin's new draft analysis of the PSP, Goldsmith agreed with Philbin's concerns about the existing legal analysis supporting the program, [redacted]

~~(S//SI//NF)~~ [redacted]

[redacted]

[redacted]

~~(TS//SI//NF)~~ Goldsmith concluded that the NSA's interception of [redacted] did not comply with FISA's requirement to obtain judicial authorization, and did not fall within any of the exceptions to this requirement. Goldsmith later wrote in a 6 May 2004 legal memorandum reassessing the legality of the program that a proper analysis of the PSP "must not consider FISA in isolation" but rather must consider whether Congress, by authorizing the use of military force against al-Qa'ida, also "effectively exempts" such surveillance from FISA. Goldsmith believed that this reading of the AUMF was correct because the AUMF authorized the President to use "all necessary and appropriate force" against the enemy that attacked the United States on 11 September 2001, and to "prevent any future acts of international terrorism against the United States" by such enemy—authority that has long been recognized to include the use of SIGINT as a military tool. Alternatively, Goldsmith reasoned that even if the AUMF did not exempt surveillance under the program from the restrictions imposed by FISA, the question was sufficiently ambiguous to warrant the application of the doctrine of constitutional avoidance, and therefore should be construed not to prohibit the activity.[11]

[redacted]

[11] ~~(TS//SI//NF)~~ [redacted]

~~(TS//SI//NF)~~ In late 2003, Philbin and Goldsmith were the only two DoJ officials in a position to brief the Attorney General and White House officials on the status of their legal reassessment and its potential ramifications for the operation of the program. Goldsmith advised Ashcroft that, despite concerns about the program, Ashcroft should certify the 9 December 2003 Presidential Authorization. Goldsmith later advised Ashcroft to certify the 14 January 2004 authorization as well. Goldsmith told us that he made these recommendations to Ashcroft with the caveat that although he believed Yoo's memorandums to be flawed, Goldsmith had not yet concluded that the program itself was illegal.

(U) Department of Justice Officials Convey Concerns About the Program to the White House

~~(TS//SI//NF)~~ In December 2003, Goldsmith and Philbin met with Addington and Gonzales at the White House to express their growing concerns about the legal underpinnings for the program. Goldsmith said he told them that OLC was not sure the program could survive in its current form. According to Goldsmith's contemporaneous notes of these events, these discussions did not contemplate an interruption of the program, although the White House officials represented that they would "agree to pull the plug" if the problems with the program were found to be sufficiently serious. Goldsmith told us that the White House—typically through Addington—told him "several times" that it would halt the program if DoJ found that it could not be legally supported.

~~(TS//SI//NF)~~ On 18 December 2003, Goldsmith met again with Addington and Gonzales and wrote in his notes that during this meeting he conveyed with "more force" his "serious doubts and the need to get more help to resolve the issue [as soon as possible]." Goldsmith told us that during this meeting he also asked to have Deputy Attorney General Comey read into the program. According to Goldsmith's notes, Addington and Gonzales "bristle[d]" at that suggestion. Goldsmith told us that he requested that Comey be read in because he believed he would need Comey's assistance to help "make the case" to the White House that the program was legally flawed. In addition, he said he wanted Comey read in because, as the Deputy Attorney General, Comey was Philbin's direct supervisor.

~~(TS//SI//NF)~~ Goldsmith's efforts to gain the White House's permission to have additional attorneys, and especially Comey, read into the program continued through January 2004. According to Goldsmith's notes, both Addington and Gonzales pressed Goldsmith on his reason for the request and continued to express doubt that additional DoJ personnel were needed. However, in late January 2004 the White House agreed to allow Comey to be read in, and Comey was briefed into the PSP on 12 March 2004 by Hayden.

~~(S//NF)~~ After his briefing, Comey discussed the program with Goldsmith, Philbin, and other DoJ officials, and agreed that the concerns with Yoo's legal analysis were well-founded.[12] Comey told us that of particular concern to him and Goldsmith was the notion that Yoo's legal analysis entailed ignoring an act of Congress, and doing so without full Congressional notification.

~~(TS//SI//NF)~~ Comey told us that in early March 2004 the sense at DoJ was that "we can get there" with regard to [redacted] albeit by using an aggressive legal analysis. However, he agreed with Goldsmith's conclusion that [redacted] would require [redacted]

(U) Conflict Between the Department of Justice and the White House Over the Program

(U) Comey told us that he met with Ashcroft for lunch on 4 March 2004 to discuss the PSP, and that Ashcroft agreed with Comey and the other DoJ officials' assessment of the potential legal problems with the program. Three hours after their lunch meeting, Ashcroft became ill and was admitted to the George Washington University Hospital.[13] On 5 March 2004, Goldsmith advised Comey by memorandum that under the circumstances of Ashcroft's medical condition and hospitalization, a "clear basis" existed for Comey to exercise the authorities of the Attorney General allowed by law as Deputy Attorney General or Acting Attorney General. The "cc" line of Goldsmith's memorandum to Comey indicated that a copy of the memorandum was sent to Gonzales.

~~(TS//SI//NF)~~ On 5 March 2004—six days before the Presidential Authorization then in effect was set to expire—Goldsmith and Philbin met with Addington and Gonzales at the White House to again convey their concerns about the PSP. [redacted] Later that day, Gonzales called Goldsmith to request a letter from OLC stating that Yoo's prior OLC opinions "covered the program." Philbin told us that Gonzales was not requesting a new opinion that the program itself was legal, but only a letter stating that the prior opinions had concluded that it was.

---

[12] ~~(TS//SI//OC/NF)~~ The other officials included Counsel for Intelligence Policy Baker, Counselor to the Attorney General Levin, and Comey's Chief of Staff Chuck Rosenberg. Both Levin and Rosenberg had been read into the PSP while at the FBI. Comey also discussed DoJ's concerns about the legality of the program with FBI Director Mueller on 1 March 2004. Mueller told us that this was the first time he had been made aware of DoJ's concerns.

[13] (U) Ashcroft's doctors did not clear Ashcroft to resume his duties as Attorney General until 31 March 2004.

~~(TS//SI//NF)~~ As a result of Gonzales's request, Goldsmith, Philbin, and Comey re-examined Yoo's memorandums with a view toward determining whether they adequately described the actual collection activities of the NSA under the Presidential Authorizations. They concluded that the memorandums did not. According to Goldsmith, the conclusion that Yoo's memorandums failed to accurately describe, let alone provide a legal analysis of, [redacted] meant that OLC could not tell the White House that the program could continue under the authority of those legal memorandums.

~~(TS//SI//NF)~~ On 6 March 2004, Goldsmith and Philbin, with Comey's concurrence, went to the White House to meet with Addington and Gonzales to convey their conclusions that [redacted] According to Goldsmith's notes, Addington and Gonzales "reacted calmly and said they would get back with us." On Sunday, 7 March 2004, Goldsmith and Philbin met again with Addington and Gonzales at the White House. According to Goldsmith, the White House officials informed Goldsmith and Philbin that they disagreed with their interpretation of Yoo's memorandums and on the need to change the scope of the NSA's collection under the PSP.

~~(S//NF)~~ On 9 March 2004, Gonzales called Goldsmith to the White House in an effort to persuade him that his criticisms of Yoo's memorandums were incorrect and that Yoo's analysis provided sufficient legal support for the program. [redacted] After Goldsmith stated that he disagreed, Gonzales next argued for a "30-day bridge" to get past the expiration of the current Presidential Authorization on 11 March 2004. Gonzales reasoned that Ashcroft, who was still hospitalized, was not in any condition to sign a renewal of the authorization, and that a "30-day bridge" would move the situation to a point where Ashcroft would be well enough to approve the program. Goldsmith told Gonzales he could not agree to recommend an extension because aspects of the program lacked legal support.

~~(TS//SI//NF)~~ At noon on 9 March, another meeting was held at the White House in Card's office. According to Mueller's notes, Mueller, Card, Vice President Cheney, Deputy Director of Central Intelligence John E. McLaughlin, Hayden, Gonzales, and other unspecified officials were present. Comey, Goldsmith, and Philbin were not invited to this meeting. After a presentation on the value of the PSP by NSA and CIA officials, it was then explained to the group that Comey "has problems" with [redacted] Mueller's notes state that the Vice President suggested that "the President may have to reauthorize without [the] blessing of DoJ," to which Mueller responded, "I could have a problem with that," and that the FBI would "have to review legality of continued participation in the program."

~~(TS//SI//NF)~~ A third meeting at the White House was held on 9 March, this time with Comey, Goldsmith, and Philbin present. Gonzales told us that the meeting was held to make sure that Comey understood what was at stake with the program and to demonstrate its value. Comey said the Vice President stressed that the program was "critically

important" and warned that Comey would risk "thousands" of lives if he did not agree to recertify it. Comey said he stated at the meeting that he, as Acting Attorney General, could support reauthorizing [redacted] provided the collection was [redacted] However, he told the group "we can't get there" on [redacted] According to Comey, the White House officials said they could not agree to that modification.

~~(S//NF)~~ Gonzales told us that after President Bush was advised of the results of the 9 March meetings, he instructed the Vice President on the morning of 10 March to call a meeting with Congressional leaders to advise them of the impasse with DoJ. That afternoon, Gonzales and other White House and IC officials, including Vice President Cheney, Card, Hayden, McLaughlin, and Tenet, convened an "emergency meeting" with Congressional leaders in the White House Situation Room. The Congressional leaders in attendance were Senate Majority and Minority Leaders William H. "Bill" Frist and Thomas A. Daschle; Senate Select Committee on Intelligence Chairman Pat Roberts and Vice Chairman John D. Rockefeller, IV; Speaker of the House J. Dennis Hastert and House Minority Leader Nancy Pelosi; and House Permanent Select Committee on Intelligence Chair Porter Goss and Ranking Member Jane Harman. No DoJ officials were asked to be present at the meeting.

~~(S//NF)~~ According to Gonzales's notes of the meeting, individual Congressional leaders expressed thoughts and concerns related to the program. Gonzales told us that the consensus was that the program should continue. Gonzales also said that following the meeting with Congressional leaders, President Bush instructed him and Card to go to the George Washington University Hospital to speak to Ashcroft, who was in the intensive care unit recovering from surgery.

(U) According to notes from Ashcroft's FBI security detail, at 18:20 on 10 March 2004, Card called the hospital and spoke with an agent in the security detail, advising the agent that President Bush would be calling shortly to speak with Ashcroft. Ashcroft's wife told the agent that Ashcroft would not accept the call. Ten minutes later, the agent called Ashcroft's Chief of Staff David Ayres at DoJ to request that Ayres speak with Card about the President's intention to call Ashcroft. The agent conveyed to Ayres Mrs. Ashcroft's desire that no calls be made to Ashcroft for another day or two. However, at 18:45, Card and the President called the hospital and, according to the agent's notes, "insisted on speaking [with Attorney General Ashcroft]." According to the agent's notes, Mrs. Ashcroft took the call from Card and the President and was informed that Gonzales and Card were coming to the hospital to see Ashcroft regarding a matter involving national security.

(U) At approximately 19:00, Ayres was advised that Gonzales and Card were on their way to the hospital. Ayres then called Comey, who at the time was being driven home by his security detail, and told Comey that Gonzales and Card were on their way to the

hospital. Comey told his driver to take him to the hospital. According to his May 2007 testimony before the Senate Judiciary Committee, Comey then called his Chief of Staff, Chuck Rosenberg, and directed him to "get as many of my people as possible to the hospital immediately." Comey next called Mueller and told him that Gonzales and Card were on their way to the hospital to see Ashcroft, and that Ashcroft was in no condition to receive visitors, much less make a decision about whether to recertify the PSP. According to Mueller's notes, Comey asked Mueller to come to the hospital to "witness [the] condition of AG." Mueller told Comey he would go to the hospital right away.

(U) Comey arrived at the hospital between 19:10 and 19:30. Comey said he began speaking to Ashcroft, and that it was not clear that Ashcroft could focus and that he "seemed pretty bad off." Goldsmith and Philbin also had been summoned to the hospital and arrived within a few minutes of each other. Comey, Goldsmith, and Philbin met briefly in an FBI "command post" that had been set up in a room adjacent to Ashcroft's room. Moments later, the command post was notified that Card and Gonzales had arrived at the hospital and were on their way upstairs to see Ashcroft. Comey, Goldsmith, and Philbin entered Ashcroft's room and, according to Goldsmith's notes, Comey and the others advised Ashcroft "not to sign anything."

(U) Gonzales and Card entered Ashcroft's hospital room at 19:35. Gonzales told us that he had with him in a manila envelope the 11 March 2004, Presidential Authorization for Ashcroft to sign. According to Philbin, Gonzales first asked Ashcroft how he was feeling. Ashcroft replied, "not well." Gonzales then said words to the effect, "You know, there's a reauthorization that has to be renewed . . .." Gonzales told us that he may also have told Ashcroft that White House officials had met with Congressional leaders "to pursue a legislative fix."

~~(TS//SI//NF)~~ Comey testified to the Senate Judiciary Committee that at this point Ashcroft told Gonzales and Card "in very strong terms" his objections to the PSP, which Comey testified Ashcroft drew from his meeting with Comey about the program a week earlier. Goldsmith's notes indicate that Ashcroft complained in particular that NSA's collection activities exceeded the scope of the authorizations and the OLC memorandums. Comey testified that Ashcroft next stated:

> "But that doesn't matter, because I'm not the Attorney General. There is the Attorney General," and he pointed to me—I was just to his left. The two men [Gonzales and Card] did not acknowledge me; they turned and walked from the room.

(U) Moments after Gonzales and Card departed, Mueller arrived at the hospital. Mueller met briefly with Ashcroft and later wrote in his notes, "AG in chair; is feeble, barely articulate, clearly stressed."

(U) Before leaving the hospital, Comey received a call from Card. Comey testified that Card was very upset and demanded that Comey come to the White House immediately. Comey told Card that he would meet with him, but not without a witness, and that he intended that witness to be Solicitor General Theodore B. Olson.

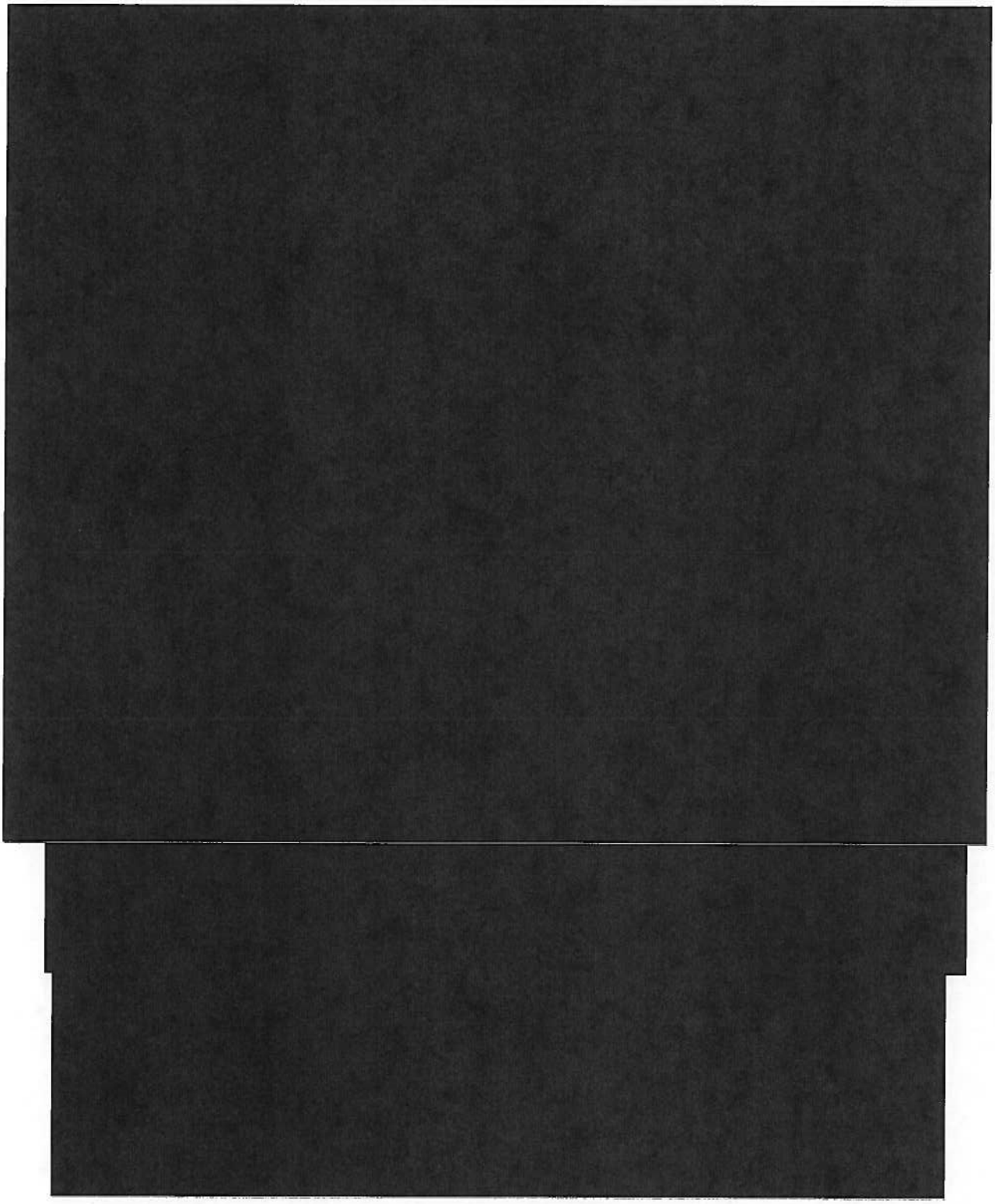
(U) Comey and the other DoJ officials left the hospital at 20:10 and met at DoJ. They were joined there by Olson. During this meeting, a call came from the Vice President for Olson, which Olson took on a secure line in Comey's office while Comey waited outside. Comey told us he believes the Vice President effectively read Olson into the program during that conversation. Comey and Olson then went to the White House at about 23:00 that evening and met with Gonzales and Card. Gonzales told us that little more was achieved at this meeting than a general acknowledgement that a "situation" continued to exist because of the disagreement between DoJ and the White House regarding the program.

~~(S//NF)~~ White House Counsel Certifies Presidential Authorization Without Department of Justice Concurrence

~~(TS//STLW//SI//OC/NF)~~ On the morning of 11 March 2004, with the Presidential Authorization set to expire, President Bush signed a new authorization for the PSP. In a departure from the past practice of having the Attorney General certify the authorization as to form and legality, the 11 March authorization was certified by White House Counsel Gonzales. The 11 March authorization also differed markedly from prior authorizations in three other respects.

~~(TS//STLW//SI//OC/NF)~~ The first significant difference between the 11 March 2004 Presidential Authorization and prior authorizations was the President's explicit assertion that the exercise of his Article II Commander-in-Chief authority [redacted]

~~(TS//STLW//SI//OC/NF)~~ Second, [redacted]



~~(TS//SI//NF)~~ The third departure from prior authorizations was the inclusion of a statement that [redacted] (Id. at para. 10.)[14]

~~(TS//SI//NF)~~ Card informed Comey by telephone on the morning of 11 March 2004 that the President had signed the new authorization that morning. At approximately 12:00, Gonzales called Goldsmith to inform him that the President, in issuing the authorization, had made an interpretation of law concerning his authorities and that DoJ should not act in contradiction of the President's determinations.

~~(TS//SI//NF)~~ Also at 12:00 on 11 March, Mueller met with Card at the White House. According to Mueller's notes, Card summoned Mueller to his office to bring Mueller up-to-date on the events of the preceding 24 hours, including the briefing of the Congressional leaders the prior afternoon and the President's issuance of the new authorization without DoJ's certification as to legality. In addition, Card told Mueller that if no "legislative fix" could be found by 6 May 2004, when the 11 March authorization was set to expire, the program would be discontinued.

~~(TS//SI//NF)~~ According to Mueller's notes, Card acknowledged to Mueller that President Bush had sent him and Gonzales to the hospital to seek Ashcroft's certification for the 11 March 2004 authorization, but that Ashcroft had said he was too ill to make the determination and that Comey was the Acting Attorney General. Mueller wrote that he told Card that the failure to have DoJ representation at the Congressional briefing and the attempt to have Ashcroft certify the authorization without going through Comey "gave the strong perception that the [White House] was trying to do an end run around the Acting [Attorney General] whom they knew to have serious concerns as to the legality of portions of the program." Card responded that he and Gonzales were unaware at the time of the hospital visit that Comey was the Acting Attorney General, and that they had only been following the directions of the President.

~~(S//NF)~~ Several senior DoJ and FBI officials, including Comey, Goldsmith, and Mueller considered resigning after the 11 March 2004 Presidential Authorization was signed without DoJ's concurrence. These officials cited as reasons for considering resignation the manner in which the White House had handled its dispute with DoJ and the treatment of Ashcroft, among other reasons.

~~(S//NF)~~ On 12 March 2004, Mueller drafted by hand a letter stating, in part: "[A]fter reviewing the plain language of the FISA statute, and the order issued yesterday by the President . . . and in the absence of further clarification of the legality of the program from the Attorney General, I am forced to withdraw the FBI from participation in the program.

---

[14] [redacted]

Further, should the President order the continuation of the FBI's participation in the program, and in the absence of further legal advice from the AG, I would be constrained to resign as Director of the FBI." Mueller told us he planned on having the letter typed and then tendering it, but that based on subsequent events his resignation was not necessary.

~~(TS//SI//NF)~~ Mueller sent Comey a memorandum seeking guidance on how the FBI should proceed in light of developments related to the Presidential Authorizations. The memorandum asked whether FBI agents detailed to the NSA to work on the PSP should be recalled; whether the FBI should continue to receive and investigate tips based on [redacted] and whether [redacted]

(U) On the morning of 12 March, Comey and Mueller attended the regular daily threat briefing with the President in the Oval Office. Comey said that, following the briefing, President Bush called him into the President's private study for an "unscheduled meeting." Comey told the President of DoJ's legal concerns regarding the PSP. According to Comey, the President's response indicated that he had not been fully informed of these concerns. Comey told the President that the President's staff had been advised of these issues "for weeks." According to Comey, the President said that he just needed until May 6 (the date of the next authorization), and that if he could not get Congress to fix FISA by then he would shut down the program. The President emphasized the importance of the program and that it "saves lives."

~~(TS//SI//NF)~~ The President next met with Mueller. According to Mueller's notes, Mueller told the President of his concerns regarding the FBI's continued participation in the program without an opinion from the Attorney General as to its legality, and that he was considering resigning if the FBI were directed to continue to participate without the concurrence of the Attorney General. The President directed Mueller to meet with Comey and other PSP principals to address the legal concerns so that the FBI could continue participating in the program "as appropriate under the law." Comey decided not to direct the FBI to cease cooperating with the NSA in conjunction with the PSP. Comey's decision is documented in a one-page memorandum from Goldsmith to Comey in which Goldsmith explained that the President, as Commander-in-Chief and Chief Executive with the constitutional duty to "take care that the laws are faithfully executed," made a determination that the PSP, as practiced, was lawful. Goldsmith concluded that this determination was binding on the entire Executive Branch, including Comey in his exercise of the powers of the Attorney General.

~~(TS//SI//NF)~~ The same day, an interagency working group was convened to continue reanalyzing the legality of the PSP. In accordance with the President's directive to Mueller, officials from the FBI, NSA, and CIA were brought into the process, although the OLC maintained the lead role. On 16 March 2004, Comey drafted a memorandum to Gonzales setting out Comey's advice to the President regarding the PSP. Comey advised that the President may lawfully continue [redacted] Comey further

wrote that DoJ remained unable to find a legal basis to support [redacted] and he advised that such [redacted] Finally, Comey cautioned that he believed the ongoing collection of [redacted] raised "serious issues" about Congressional notification, "particularly where the legal basis for the program is the President's decision to assert his authority to override an otherwise applicable Act of Congress."

(U) Gonzales replied by letter on the evening of 16 March. The letter stated, in part:

> Your memorandum appears to have been based on a misunderstanding of the President's expectations regarding the conduct of the Department of Justice. While the President was, and remains, interested in any thoughts the Department of Justice may have on alternative ways to achieve effectively the goals of the activities authorized by the Presidential Authorization of March 11, 2004, the President has addressed definitively for the Executive Branch in the Presidential Authorization the interpretation of the law.

~~(TS//SI//NF)~~ White House Agrees to [redacted]

~~(TS//SI//NF)~~ Notwithstanding Gonzales's letter, on 17 March 2004 the President decided to [redacted] The President's directive was expressed in two modifications to the 11 March 2004 Presidential Authorization.

~~(TS//STLW//SI//OC/NF)~~ On 19 March 2004, the President signed, and Gonzales certified as to form and legality, a modification of the 11 March 2004 Presidential Authorization. The modification made two significant changes to the current authorization and a third important change affecting all subsequent authorizations. First, the modification [redacted] Second, the modification [redacted]

[redacted] Third, the modification authorized [redacted]

~~(TS//STLW//SI//OC/NF)~~ On 2 April 2004, President Bush signed, and Gonzales certified as to form and legality, a second modification of the 11 March 2004, Presidential Authorization. This modification addressed only [redacted] of the PSP. [redacted]

~~(S//NF)~~ On 6 May 2004, Goldsmith and Philbin completed an OLC legal memorandum assessing the legality of the PSP as it was then operating. The memorandum stated that the AUMF passed by Congress shortly after the attacks of 11 September 2001 gave the President authority to use both domestically and abroad "all necessary and appropriate force," including SIGINT capabilities, to prevent future acts of international terrorism against the United States. According to the memorandum, the AUMF was properly read as an express authorization to conduct targeted electronic surveillance against al-Qa'ida and its affiliates, the entities responsible for attacking the United States, thereby supporting the President's directives to conduct these activities under the PSP. Much of the legal reasoning in the 6 May 2004 OLC memorandum was publicly released by DoJ in a "White Paper"—"Legal Authorities Supporting the Activities of the National Security Agency Described by the President"—issued on 19 January 2006 after the content

[redacted]

collection portion of the program was revealed in *The New York Times* and publicly confirmed by the President in December 2005.

(U) Restrictions on Access to the President's Surveillance Program Impeded Department of Justice Legal Review

~~(TS//SI//OC/NF)~~ The DoJ IG found it extraordinary and inappropriate that a single DoJ attorney, John Yoo, was relied upon to conduct the initial legal assessment of the PSP, and that the lack of oversight and review of Yoo's work, which was contrary to the customary practice of OLC, contributed to a legal analysis of the PSP that, at a minimum, was factually flawed. Deficiencies in the legal memorandums became apparent once additional DoJ attorneys were read into the program in 2003 and those attorneys sought a greater understanding of the PSP's operation. The White House's strict controls over access to the PSP undermined DoJ's ability to provide the President the best available advice about the program. The DoJ IG also concluded that the circumstances plainly called for additional DoJ resources to be applied to the legal review of the program, and that it was the Attorney General's responsibility to be aware of this need and to take steps to address it. However, the DoJ OIG could not determine whether Ashcroft aggressively sought additional read-ins to assist with DoJ's legal review of the program prior to 2003 because Ashcroft did not agree to be interviewed.

(U) TRANSITION OF PRESIDENT'S SURVEILLANCE PROGRAM ACTIVITIES TO FOREIGN INTELLIGENCE SURVEILLANCE ACT AUTHORITY

~~(TS//SI//NF)~~ Internet Metadata Collection Transition to Operation Under FISA Authority

~~(TS//SI//OC/NF)~~ [redacted]

~~(TS//SI//NF)~~ The government's FISA application, entitled "Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes," was filed [redacted] The application package included:

- A proposed order authorizing the collection activity and secondary orders mandating carriers to cooperate.
- A declaration by Hayden explaining the technical aspects of the proposed Internet metadata collection and identifying the government official

seeking to use the pen register and trap and trace (PR/TT) devices covered by the application for purposes of 50 U.S.C. § 1842(c)(1).

- A declaration by Tenet describing the threat posed by [redacted] to the United States.
- A certification from Ashcroft stating that the information likely to be obtained from the PR/TT devices was relevant to an ongoing investigation to protect against international terrorism, as required by 50 U.S.C. § 1842(c).
- A memorandum of law and fact in support of the application.

~~(TS//SI//OC/NF)~~ The objective of the application was to secure authority under FISA to collect [redacted] bulk Internet metadata [redacted] DoJ constructed its legal argument for this novel use of PR/TT devices around traditional authorities provided under FISA. (See 50 U.S.C. § 1842(a)(1).) The government argued that the NSA's proposed collection of metadata met the requirements of FISA by noting that the metadata sought comported with the "dialing, routing, addressing, or signaling information" type of data described in FISA's definitions of PR/TT devices. (See 18 U.S.C. § 3127(3) and (4).) The government next argued that the information likely to be obtained from the PR/TT devices was relevant to an ongoing investigation to protect against international terrorism, as certified by the Attorney General under 50 U.S.C. § 1842(c). In support of this "certification of relevance" the government stated that the FBI [redacted] The government also stated that the NSA needed to collect metadata in bulk to effectively perform contact chaining [redacted] that would enable the NSA to discover enemy communications.

~~(TS//SI//NF)~~ The application requested that the NSA be authorized to collect metadata [redacted] The application represented that for most of the proposed collection on [redacted] it was "overwhelmingly likely" that at least one end of the transmitted communication either originated in or was destined for locations outside the United States, and that in some cases both ends of the communication were entirely foreign. However, the government acknowledged that [redacted]

~~(TS//SI//NF)~~ The application proposed allowing 10 NSA analysts access to the database. The NSA analysts were to be briefed by NSA OGC personnel concerning the circumstances under which the database could be queried, and all queries would have to be

approved by one of seven senior NSA officials. The application proposed that queries of the Internet metadata archive would be performed when the Internet communication address met the following standard:

> [B]ased on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known e-mail address is associated with [redacted]

~~(TS//SI//OC/NF)~~ The application and supporting documents explained that the NSA intended to use the Internet metadata to develop contact chaining [redacted] The NSA estimated that its queries of the database would generate approximately 400 tips to the FBI and CIA each year. Of these tips, the NSA projected that 25 percent would include U.S. person information, amounting to leads including information on about "four to five U.S. persons each month."

~~(TS//SI//NF)~~ On 14 July 2004, Kollar-Kotelly signed a Pen Register and Trap and Trace Opinion and Order (PR/TT Order) based on her findings that the proposed collection of Internet metadata and the government's proposed controls over and dissemination of this information satisfied the requirements of FISA. The PR/TT Order, which granted the government's application in all key respects, approved for a period of 90 days the collection within the United States of Internet metadata [redacted]

~~(TS//SI//NF)~~ The PR/TT Order also required the government to comply with certain additional restrictions and procedures either adapted from or not originally proposed in the application. The FISC amended the government's proposed querying standard, consistent with 50 U.S.C. § 1842(c)(2), to include the proviso that the NSA may query the database based on its reasonable articulable suspicion that a particular known Internet communication address is associated with [redacted] "provided, however, that an [redacted] believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution." Regarding the storing, accessing, and disseminating of the Internet metadata obtained by the NSA, the FISC ordered that the NSA store the information in a manner that ensures it is not commingled with other data, and "generate a log of auditing information for each occasion when the information is accessed, to include the ... retrieval request." The FISC also issued separate orders to [redacted] service providers [redacted] to assist the NSA with the installation and use of the PR/TT devices and to maintain the secrecy of the NSA's activities.

~~(TS//SI//NF)~~ Several officials told us that obtaining the PR/TT Order was seen as a great success, and that there was general agreement that the government had secured all the authority it sought to conduct the bulk Internet metadata collection.

~~(TS//SI//NF)~~ The FISC first renewed the PR/TT Order on [redacted] and then renewed it by subsequent orders at approximately 90-day intervals. In these renewals, the FISC [redacted] that it approved with the 14 July 2004 PR/TT Order. Under the PR/TT renewal applications, the scope of authorized queries against the PR/TT database remained limited to queries that concerned [redacted]

(U) Department of Justice Notices of Compliance Incidents

~~(TS//SI//NF)~~ On [redacted] DoJ OIPR filed a Notice of Compliance Incidents with the FISC describing certain "unauthorized collection" that had taken place following issuance of the PR/TT Order. [redacted]

~~(TS//SI//NF)~~ On [redacted] the FISC issued a Compliance Order stating that the "NSA violated its own proposed limitations." The FISC stated that it was troubled by the duration of the violations, which extended from 14 July through [redacted] and that the Court was reluctant to issue a renewal of the PR/TT Order as to [redacted] However, Kollar-Kotelly signed a Renewal Order on [redacted] allowing the NSA to continue collecting Internet metadata under FISA on terms similar to the original PR/TT Order. [redacted]

[redacted]

~~(TS//SI//NF)~~ Telephony Metadata Collection Transition to Operation Under FISA Authority

~~(TS//SI//NF)~~ Another part of the PSP, bulk collection of telephony metadata, was brought under FISA authority in May 2006. As with Internet metadata, the bulk nature of the telephony metadata collection provided the NSA the ability to conduct contact chaining [redacted]

~~(TS//SI//NF)~~ The transition of bulk telephony metadata collection from Presidential authority to FISA authority relied on a provision in FISA that authorized the FBI to seek an order from the FISC compelling the production of "any tangible things" from any business, organization, or entity, provided the items are for an authorized investigation to protect against international terrorism or clandestine intelligence activities. (See 50 U.S.C. § 1861.) Orders under this provision are commonly referred to as "Section 215" orders in reference to Section 215 of the USA PATRIOT Act, which amended the "business records" provision in Title V of FISA.[18] The "tangible things" sought in this Section 215 application were the telephone call detail records of certain telecommunications service providers.

~~(TS//SI//NF)~~ The timing of the decision in May 2006 to seek a FISC order for the bulk collection of telephony metadata was driven primarily by external events. A 16 December 2005 article in *The New York Times* entitled, "Bush Lets U.S. Spy on Callers Without Courts," described in broad terms the content collection aspect of the PSP. [redacted] On 17 December 2005, in response to the article, President Bush publicly confirmed that he had authorized the NSA to intercept the international communications of people with known links to al-Qa'ida and related terrorist organizations. On 19 January 2006, DoJ issued its White Paper—"Legal Authorities Supporting the Activities of the National Security Agency Described by the President"—that addressed in an unclassified form the legal basis for the collection activities described in *The New York Times* article and confirmed by the President.

[18] (U) Prior to the enactment of Section 215 of the USA PATRIOT Act, the FISA "business records" provisions were limited to obtaining information about a specific person or entity under investigation and only from common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities.

~~(TS//SI//NF)~~ According to Bradbury, the head of OLC at that time, the legal analysis contained in the White Paper [redacted] Although *The New York Times* article did not describe this aspect of the PSP, reporters at *USA Today* asked about this aspect of the program in early 2006. Bradbury [redacted] anticipated that a *USA Today* article would attract significant public attention when published. As anticipated, on 11 May 2006, the *USA Today* published the results of its investigation in an article entitled, "NSA Has Massive Database of American Phone Calls."

~~(TS//SI//NF)~~ On 23 May 2006, the FBI filed with the FISC a Section 215 application seeking authority to collect telephony metadata to assist the NSA in finding and identifying members or agents of [redacted] in support of the [redacted] FBI investigations then pending and other IC operations. The application requested an order compelling certain telecommunications companies to produce (for the duration of the 90-day order) call detail records relating to all telephone communications maintained by the carriers. According to the application, the majority of the telephony metadata provided to the NSA was expected to involve communications that were (1) between domestic and foreign locations, or (2) wholly within the United States, including local telephone calls. The application estimated that the collection would involve the NSA receiving approximately [redacted] call detail records per day.[19]

~~(TS//SI//NF)~~ The application acknowledged that the vast collection would include communications records of U.S. persons located within the United States who were not the subject of any FBI investigation. However, relying on the precedent established by the PR/TT Order, the application asserted that the collection was needed for the NSA to find [redacted] and to identify unknown operatives, some of whom may be in the United States or in communication with U.S. persons, by using contact chaining [redacted] As was done under the PSP, the call detail records would be entered in an NSA database and analysts would query the data with particular telephone numbers to identify connections with other numbers [redacted] The proposed query standard in the Section 215 application essentially was the same standard applied under the PSP in connection with telephony metadata, and the same standard the FISC authorized in the PR/TT Order for Internet metadata. The Section 215 application also included in the proposed query standard the First Amendment proviso that the FISC added to the PR/TT query standard.

---

[19] ~~(TS//SI//NF)~~ The actual average amount of telephony metadata collected per day is [redacted] call detail records rather than [redacted] estimated in the application.

~~(TS//SI//NF)~~ On 24 May 2006, the FISC approved the Section 215 application, finding that there were reasonable grounds to believe that the telephony metadata records sought were relevant to authorized investigations the FBI was conducting to protect against international terrorism. The FISC Section 215 order incorporated each of the procedures proposed in the government's application relating to access to and use of the metadata, which were nearly identical to those included in the Internet metadata PR/TT Order.

~~(TS//SI//NF)~~ Through March 2009, the FISC renewed the authorities granted in the 24 May 2006 order at approximately 90-day intervals, with some modifications sought by the U.S. government. For example, the FISC granted an August 2006 motion requesting [redacted] Except for these and other minor modifications, the terms of the FISC's grant of Section 215 authority for the bulk collection of telephony metadata remained essentially unchanged from the first approval in May 2006 until March 2009. [redacted] Further, the FISC's Section 215 Orders did not require the NSA to modify its use of the telephony metadata from an analytical perspective. NSA analysts were authorized to query the data as they had under the PSP, conduct metadata analysis, and disseminate the results to the FBI, the CIA, and other customers.

~~(TS//SI//NF)~~ However, the FISC drastically changed the authority contained in its March 2009 Section 215 Order after it was notified in January 2009 that the NSA had been querying the metadata in a manner that was not authorized by the court's Section 215 Orders. Specifically, the NSA, on a daily basis, was automatically querying the metadata with [redacted] telephone numbers from an alert list that had not been determined to satisfy the reasonable articulable suspicion standard required by the FISC to access the telephony metadata for search or analysis purposes.

~~(TS//SI//NF)~~ On 2 March 2009, the FISC issued an order that addressed the compliance incidents that had been reported in January 2009, the government's explanation for their occurrence, and the remedial and prospective measures being taken in response. The FISC stated its concerns with the telephony metadata program and its lack of confidence "that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders." Nonetheless, the FISC authorized the government to continue collecting telephony metadata under the Section 215 Orders. The FISC explained that in light of the government's repeated representations that the collection of the telephony metadata is vital to national security, taken together with the court's prior determination that the collection properly administered conforms with the FISA statute, that "it would not be prudent" to order the government to cease the bulk collection.

~~(TS//SI//NF)~~ However, believing that "more is needed to protect the privacy of U.S. person information acquired and retained" pursuant to the Section 215 Orders, the FISC prohibited the government from accessing the metadata collected "until such time as the government is able to restore the Court's confidence that the government can and will comply with previously approved procedures for accessing such data." The government may, on a case-by-case basis, request authority from the FISC to query the metadata with a specific telephone number to obtain foreign intelligence. The FISC also authorized the government to query the metadata without court approval to protect against an imminent threat to human life, provided the government notifies the court within the next business day.

~~(TS//SI//NF)~~ Content Collection Transition to Operation Under FISA Authority

~~(TS//SI//NF)~~ The last part of the PSP brought under FISA authority was telephone and Internet communications content collection. As explained below, the effort to accomplish this transition was legally and operationally complex and required an enormous effort on the part of the government and the FISC. The FISC judge who ruled on the initial application approved the unconventional legal approach the government proposed to fit PSP's content collection activities within FISA. However, the FISC judge responsible for considering the government's renewal application rejected the legal approach. This resulted in significant diminution in authorized surveillance activity involving content collection and hastened the enactment of legislation that significantly amended FISA and provided the government surveillance authorities broader than those authorized under the PSP.

[redacted]

~~(TS//SI//NF)~~ The government filed the content collection application with the FISC on 13 December 2006. The application sought authority to intercept the content of telephone and electronic communications of [redacted] The application sought to replace the conventional practice under FISA of filing individual applications each time the government had probable cause to believe that a particular telephone number or Internet communication address was being used or about to be used by members or agents of a foreign power. In the place of the individualized process, the application proposed that the FISC establish broad parameters for the interception of communications—the groups that can be targeted and the locations where the surveillance can be conducted—and that NSA officials, rather than FISC judges, determine within these parameters the particular selectors to be collected against. [redacted]

[redacted] albeit with FISC review and supervision. The government's approach in the FISA application rested on a broad interpretation of the statutory term "facility" and the use of minimization procedures by NSA officials to make probable cause determinations about individual selectors, rather than have a FISC judge make such determinations.

~~(TS//SI//NF)~~ In short, the government's content application asked the FISC to find probable cause to believe that [redacted] engaged in international terrorism, and that [redacted] Then, within these parameters, NSA officials would make probable cause findings (subsequently reviewed by the FISC) about whether individual telephone numbers or Internet communications addresses are used by members or agents of [redacted] and whether the communications of those numbers and addresses are to or from a foreign country. When probable cause findings were made, the NSA could direct the telecommunications companies to provide the content of communications associated with those telephone numbers and Internet communications addresses.

~~(TS//STLW//SI//OC/NF)~~ On 10 January 2007, Judge Malcolm J. Howard approved the government's 13 December 2006 content application as it pertained to foreign selectors—telephone numbers and Internet communications addresses reasonably believed to be used by individuals outside the United States. The effort to implement the order was a massive undertaking for DoJ and NSA. At the time of the order, the NSA was actively tasking for content collection approximately [redacted] foreign selectors—Internet communications addresses or telephone numbers—under authority of the PSP. Approximately [redacted] of these were filed with Howard on an approved schedule of rolling submissions over the 90-day duration of the order.

~~(TS//SI//NF)~~ However, Howard did not approve the government's 13 December 2006 content application as it pertained to domestic selectors—telephone numbers and Internet communications addresses reasonably believed to be used by individuals in the United States. Howard advised DoJ to file a separate application for the international calls of domestic selectors that took a more traditional approach to FISA. A more traditional approach meant that the facilities targeted by the FISA application should be particular telephone numbers and Internet communication addresses and that the probable cause determination for a particular selector would reside with the FISC. DoJ did this in an application filed on 9 January 2007, which Howard approved the following day. The FISC renewed the domestic selectors order approved by Howard for the final time in [redacted] and it has since expired.

~~(TS//SI//NF)~~ DoJ's first renewal application to extend the foreign selectors authorities was filed on 20 March 2007 with Judge Roger Vinson, the FISC duty judge that week. On 29 March 2007, Vinson orally advised DoJ that he could not approve the application and, on 3 April 2007, he issued an order and Memorandum Opinion explaining the reasoning for his conclusion. Vinson wrote that DoJ's foreign selectors renewal application concerns an "extremely important issue" regarding who may make probable cause findings that determine the individuals and the communications that can be subjected to electronic surveillance under FISA. In Vinson's view, the question was whether probable cause determinations are required to be made by the FISC through procedures established by statute, or whether the NSA may make such determinations under an alternative mechanism cast as "minimization procedures." Vinson concluded, based on past practice under FISA and the Congressional intent underlying the statute, that probable cause determinations must be made by the FISC.

~~(TS//SI//NF)~~ Vinson also wrote that he was mindful of the government's argument that the government's proposed approach to foreign selectors was necessary to provide or enhance the "speed and flexibility" with which the NSA responds to threats, and that foreign intelligence information may be lost in the time it takes to obtain Attorney General emergency authorizations. However, in Vinson's view, FISA's requirements reflected a balance struck by Congress between privacy interests and the need to obtain foreign intelligence information, and until Congress took legislative action on FISA to respond to the government's concerns, the FISC must apply the statute's procedures. He concluded that the government's application sought to strike a different balance for the surveillance of foreign telephone numbers and Internet communications addresses. Vinson rejected this position, stating, "the [FISA] statute applies the same requirements to surveillance of facilities used overseas as it does to surveillance of facilities used in the United States." Vinson suggested that, "Congress should also consider clarifying or modifying the scope of FISA and of this Court's jurisdiction with regard to such facilities . . .." Vinson's suggestion was a spur to Congress to consider FISA modernization legislation in the summer of 2007.

~~(TS//STLW//SI//OC/NF)~~ In May 2007, DoJ filed, and Vinson approved, a revised foreign selectors application that took a more traditional approach to FISA. Although the revised approach sought to preserve some of the "speed and agility" the government had under Howard's order, the comparatively laborious process for targeting foreign selectors under Vinson's order caused the government to place only a fraction of the desired foreign selectors under coverage. The number of foreign selectors on collection dropped from abou[redacted] under the January 2007 order to about [redacted] under the May 2007 order. The situation accelerated the government's efforts to obtain legislation that would amend FISA to address the government's surveillance capabilities within the United States directed at persons located outside the United States. The Protect America Act, signed into law on 5 August 2007, accomplished this objective by authorizing the NSA to intercept inside the United States any communications of non-U.S. persons reasonably believed to be located outside the United States, provided a significant purpose of the acquisition pertains to foreign intelligence. The Protect America Act effectively superseded Vinson's foreign

selectors order and the government therefore did not seek to renew the order when it expired on 24 August 2007.

~~(TS//SI//NF)~~ The DOJ IG concluded that several considerations favored initiating PSP's transition from Presidential authority to FISA authority earlier than March 2004, especially as the program became less a temporary response to the September 11 terrorist attacks and more a permanent surveillance tool. These considerations included PSP's substantial effect on privacy interests of U.S. persons, the instability of the legal reasoning on which the program rested for several years, and the substantial restrictions placed on FBI agents' and analysts' access to and use of program-derived information due to the highly classified status of the PSP. The DOJ IG also recommended that DoJ carefully monitor the collection, use, and retention of the information that is now collected under FISA authority and, together with other agencies, continue to examine its value to the government's ongoing counterterrorism efforts.

(U) IMPACT OF THE PRESIDENT'S SURVEILLANCE PROGRAM ON INTELLIGENCE COMMUNITY COUNTERTERRORISM EFFORTS

(U) Senior Intelligence Community Officials Believe That the President's Surveillance Program Filled an Intelligence Gap

~~(TS//SI//NF)~~ Hayden, Goss, McLaughlin, and other senior IC officials we interviewed told us that the PSP addressed a gap in intelligence collection. The IC needed increased access to international communications that transited domestic U.S. communication wires, particularly international communications that originated or terminated within the United States. However, collection of such communications required authorization under FISA, and there was widespread belief among senior IC officials that the process for obtaining FISA authorization was too cumbersome and time consuming to address the current threat. [redacted] During the May 2006 Senate hearing on his nomination to be Director of the CIA, Hayden said that, had PSP been in place before the September 2001 attacks, hijackers Khalid Almihdhar and Nawaf Alhazmi almost certainly would have been identified and located.

~~(TS//SI//OC/NF)~~ According to senior NSA officials, the PSP gave NSA the capability to exploit a key terrorist vulnerability. [redacted] With PSP authority, NSA could collect communications between terrorists in the United States and members of al-Qa'ida [redacted] located in foreign countries. The PSP provided SIGINT coverage at the seam between foreign and

domestic intelligence collection. Hayden cited as an important consequence of the PSP the NSA's ability to collect more [redacted]

~~(S//NF)~~ Hayden told us that he always felt the PSP was worthwhile and successful. His expectation was that the CIA and the FBI would be customers of program-derived information and integrate it into their respective operations. [redacted] Hayden told us that the program helped to determine that terrorist cells were not embedded within the United States to the extent that had been feared.

(U) Difficulty in Assessing the Impact of the President's Surveillance Program

~~(S//SI//NF)~~ It was difficult to assess the overall impact of PSP on IC counterterrorism efforts. Except for the FBI, IC organizations that participated in the PSP did not have systematic processes for tracking how PSP reporting was used. [redacted] We were repeatedly told that the PSP was one of a number of intelligence sources and analytic tools that were available to IC personnel, and that, because PSP reporting was used in conjunction with reporting from other intelligence sources, it was difficult to attribute the success of particular counterterrorism operations exclusively to the PSP.

(U) Impact of the President's Surveillance Program on FBI Counterterrorism Efforts

~~(S//NF)~~ The DoJ IG found it difficult to assess or quantify the impact of the PSP on FBI counterterrorism efforts. However, based on our interviews of FBI managers and agents and our review of documents, we concluded that, although PSP information had value in some counterterrorism investigations, the program generally played a limited role in the FBI's overall counterterrorism efforts. Several officials we interviewed suggested that the program provided an "early warning system" to allow the IC to detect potential

terrorist attacks, even if the program had not specifically uncovered evidence of preparations for such attacks.

(U) FBI Efforts to Assess the Value of the Program

~~(TS//SI//NF)~~ The FBI made several attempts to assess the value of the PSP to FBI counterterrorism efforts. In 2004 and again in 2006, FBI's Office of General Counsel (OGC) attempted to assess the value to the FBI of PSP information. This first assessment relied on anecdotal information and informal feedback from FBI field offices. The 2006 assessment was limited to the aspect of the PSP disclosed in *The New York Times* article and subsequently confirmed by the President, i.e., content collection.

~~(S//NF)~~ The FBI undertook two more efforts to study PSP's impact on FBI operations in early 2006. In both of these statistical studies, the FBI sought to determine what percentage of PSP tippers resulted in "significant contribution[s] to the identification of terrorist subjects or activity on U.S. soil." The FBI considered a tipper significant if it led to any of three investigative results: the identification of a terrorist, the deportation from the United States of a suspected terrorist, or the development of an asset that can report about the activities of terrorists.

~~(TS//SI//OC/NF)~~ The first study examined a sample of leads selected from the [redacted] tippers the NSA provided the FBI from approximately October 2001 to December 2005. The study found that 1.2 percent of the leads made significant contributions, as defined above. The study extrapolated this figure to the entire population of leads and determined that one could expect to find that [redacted] leads made significant contributions to FBI counterterrorism efforts. The second study, which reviewed all of the [redacted] leads the NSA provided the FBI from August 2004 through January 2006, identified no instances of significant contributions to FBI counterterrorism efforts. The studies did not include explicit conclusions on the program's usefulness. However, based in part on the results of the first study, FBI executive management, including Mueller and Deputy Director John Pistole, concluded that the PSP was "of value."

(U) FBI Judgmental Assessments of the Program

~~(S//NF)~~ We interviewed FBI headquarters and field office personnel who regularly handled PSP information for their assessments of the impact of program information on FBI counterterrorism efforts. The FBI personnel we interviewed were generally supportive of the PSP as "one tool of many" in the FBI's anti-terrorism efforts that "could help move cases forward". Even though most leads were determined not to have any connection to terrorism, many of the FBI officials believed the mere possibility of a terrorist connection made investigating the tips worthwhile.

~~(S//NF)~~ However, the exceptionally compartmented nature of the program created some frustration for FBI personnel. Some agents criticized PSP reports for providing insufficient details about the foreign individuals allegedly involved in terrorism. Others occasionally were frustrated by the prohibition on using [redacted] information in judicial processes, such as in FISA applications, although none of the FBI field office agents we interviewed could identify an investigation in which the restrictions adversely affected the case. Agents who managed counterterrorism programs at the FBI field offices we visited were critical of the [redacted] project for failing to adequately prioritize threat information and, because of the program's special status, for limiting the managers' ability to prioritize the leads in the manner they felt was warranted by the information.

~~(S//NF)~~ Mueller told us that the PSP was useful. He said the FBI must follow every lead it receives in order to prevent future terrorist attacks and that to the extent such information can be gathered and used legally it must be exploited. He stated that he "would not dismiss the potency of a program based on the percentage of hits." Mueller added that, as a general matter, it is very difficult to quantify the effectiveness of an intelligence program without "tagging" the leads that are produced in order to evaluate the role the program information played in any investigation.

(U) Impact of the President's Surveillance Program on CIA Counterterrorism Operations

(U) The CIA Did Not Systematically Assess the Effectiveness of the Program

~~(S//NF)~~ The CIA did not implement procedures to systematically assess the usefulness of the product of the PSP and did not routinely document whether particular PSP reporting had contributed to successful counterterrorism operations. CIA officials, including Hayden, told us that PSP reporting was used in conjunction with reporting from other intelligence sources; consequently, it is difficult to attribute the success of particular counterterrorism operations exclusively to the PSP. In a May 2006 briefing to the SSCI, the Deputy Director, [redacted] said that PSP reporting was rarely the sole basis for an intelligence success, but that it frequently played a supporting role. He went on to state that the program was an additional resource to enhance the CIA's understanding of terrorist networks and to help identify potential threats to the homeland. Other [redacted] officials we interviewed said that the PSP was one of many tools available to them, and that the tools were often used in combination.

~~(S//NF)~~ [redacted] However, because there is no means to comprehensively track how PSP information was used, CIA officials were able to provide

only limited information on how program reporting contributed to successful operations, and the CIA IG was unable to independently draw any conclusion on the overall usefulness of the program to CIA.

[redacted]

(U) Several Factors Hindered CIA Utilization of the Program

~~(S//NF)~~ The CIA IG concluded that several factors hindered the CIA in making full use of the capabilities of the PSP. Many CIA officials told us that too few CIA personnel at the working level were read into the PSP. At the program's inception, a disproportionate number of the CIA personnel who were read into the PSP were senior CIA managers. [redacted] the disparity between the number of senior CIA managers read into PSP and the number of working-level CIA personnel read into the program resulted in too few CIA personnel to fully utilize PSP information for targeting and analysis.

~~(S//NF)~~ [redacted] working-level CIA analysts and targeting officers who were read into the PSP had too many competing priorities, and too many other information sources and analytic tools available to them, to fully utilize PSP. [redacted] officials also told us that much of the PSP reporting was vague or without context, which led analysts and targeting officers to rely more heavily on other information sources and analytic tools, which were more easily accessed and timely than the PSP.

~~(S//NF)~~ CIA officers said that the PSP would have been more fully utilized if analysts and targeting officers had obtained a better understanding of the program's capabilities. There was no formal training on the use of the PSP beyond the initial read in to the program. Many CIA officers we interviewed said that the instruction provided in the read-in briefing was not sufficient and that they were surprised and frustrated by the lack of additional guidance. Some officers told us that there was insufficient legal guidance on the use of PSP-derived information.

~~(S//NF)~~ The factors that hindered the CIA in making full use of the PSP might have been mitigated if the CIA had designated an individual at an appropriate level of managerial authority, who possessed knowledge of both the PSP and CIA counterterrorism activities, to be responsible and accountable for overseeing CIA participation in the

program. [redacted]

(U) Impact of the President's Surveillance Program on NCTC Counterterrorism Efforts

~~(S//NF)~~ [redacted] NCTC analysts characterized the PSP as a useful tool, but they also noted that the program was only one of several valuable sources of information available to them. In their view, PSP-derived information was not of greater value than other sources of intelligence. Although NCTC analysts we interviewed could not recall specific examples where PSP information provided what they considered actionable intelligence, they told us they remember attending meetings where the benefits of the PSP were regularly discussed.

(U) Counterterrorism Operations Supported by the President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ Our efforts to independently identify how PSP information impacted terrorism investigations and counterterrorism operations were hampered by the nature of these activities, which as previously stated, frequently are predicated on multiple sources of information. Many IC officials we interviewed had difficulty citing specific instances where PSP reporting contributed to a counterterrorism success. The same handful of cases tended to be cited as PSP successes by personnel we interviewed from each of the participating IC organizations and in reports, briefing charts, and other documents we reviewed. [redacted] These cases, and others identified to us as PSP successes, are discussed below.

~~(TS//STLW/SI//OC/NF)~~ Among the more significant PSP successes was [redacted]

~~(TS//STLW/SI//OC/NF)~~ In [redacted] the FBI arrested [redacted] and [redacted] later pled guilty to [redacted] After [redacted] arrest, [redacted] provided valuable information to the law enforcement and intelligence communities. [redacted] NSA Director Alexander cited reporting on [redacted] as the most significant success of the PSP. Alexander said that PSP reporting on [redacted] "probably saved more lives" than any other PSP information produced by NSA.

~~(TS//STLW/SI//OC/NF)~~ An [redacted] tipper, dated [redacted] reported that [redacted] Additional [redacted] reporting, in [redacted] provided telephone contacts between and among [redacted] and several individuals with suspected terrorist ties located in [redacted] The FBI learned more about [redacted] ties to terrorist groups from evidence seized [redacted] evidence gathered through several interviews [redacted] The FBI arrested [redacted] on [redacted] and [redacted] was indicted on [redacted] was convicted on [redacted] on [redacted] and was sentenced to [redacted] prison term. [redacted]

~~(TS//STLW//SI//OC/NF)~~ In an undated summary of PSP successes, the NSA characterized as:

[redacted]

~~(TS//STLW//SI//OC/NF)~~ Other examples of PSP successes cited in IC records and briefings include the cases. PSP analysis and reporting helped to identify and locate who was arrested in Subsequent PSP analysis of identified This information generated several leads for the FBI.

~~(TS//STLW//SI//OC/NF)~~ According to internal FBI briefing materials, PSP reporting was "instrumental in becoming the subject of a Full Investigation." However, the FBI's Counterterrorism Division told the DoJ OIG that "no reporting factored into investigation." PSP reporting assisted in locating his network's worldwide associates

[redacted]

(U) ATTORNEY GENERAL GONZALES'S TESTIMONY ON THE PRESIDENT'S SURVEILLANCE PROGRAM

(U) As part of this review, the DoJ IG examined whether Attorney General Gonzales made false, inaccurate, or misleading statements to Congress related to the PSP. Aspects of the PSP were first disclosed publicly in a series of articles in *The New York Times* in December 2005. In response, the President publicly confirmed a portion of the PSP—which he called the terrorist surveillance program—describing it as the interception of the content of international communications of people reasonably believed to have links to al-Qaeda and related organizations. Subsequently, Gonzales was questioned about NSA surveillance activities in two hearings before the Senate Judiciary Committee in February 2006 and July 2007.

~~(S//NF)~~ Through media accounts and Comey's Senate Judiciary Committee testimony in May 2007, it was publicly revealed that DoJ and the White House had a major disagreement related to the PSP, which brought several senior DoJ and FBI officials to the brink of resignation in March 2004. In his testimony before the Senate Judiciary Committee, Gonzales stated that the dispute at issue between DoJ and the White House did not relate to the "Terrorist Surveillance Program" that the President had confirmed, but rather pertained to other intelligence activities. We believe this testimony created the misimpression that the dispute concerned activities entirely unrelated to the terrorist surveillance program, which was not accurate. In addition, we believe Gonzales's testimony that DoJ attorneys did not have "reservations" or "concerns" about the program the "President has confirmed" was incomplete and confusing [redacted] and that these concerns had been conveyed to the White House over a period of months before the issue was resolved.

~~(S//NF)~~ The DoJ IG recognizes that Gonzales was in the difficult position of testifying about a highly classified program in an open forum. However, Gonzales, as a participant in the March 2004 dispute between DoJ and the White House and, more importantly, as the nation's chief law enforcement officer, had a duty to balance his obligation not to disclose classified information with the need not to be misleading in his testimony. Although we believe that Gonzales did not intend to mislead Congress, we believe his testimony was confusing, inaccurate, and had the effect of misleading those who were not knowledgeable about the program.

(U) CONCLUSIONS

(U) Pursuant to Title III of the FISA Amendments Act of 2008, the Inspectors General of the DoD, the DoJ, the CIA, the NSA, and the ODNI conducted reviews of the PSP. In this report and the accompanying individual reports of the participating IGs, we describe how, following the terrorist attacks of 11 September 2001, the President enhanced the NSA's SIGINT collection authorities in an effort to "detect and prevent acts of terrorism against the United States."

~~(TS//SI//NF)~~ Pursuant to this authority, the NSA, [redacted] collected significant new information, such as the content of communications into and out of the United States, where one party to the communication was reasonably believed to be a member of al-Qa'ida, or its affiliates, or a group the President determined was in armed conflict with the United States. In addition, the President authorized the collection of significant amounts of telephony and Internet metadata. The NSA analyzed this information for dissemination as leads to the IC, principally the CIA and the FBI. As described in the IG reports, the scope of this collection authority changed over the course of the PSP.

(U//~~FOUO~~) The IG reports describe the role of each of the participating agencies in the PSP, including the NSA's management and oversight of the collection, analysis, and reporting process; the CIA's and FBI's use of the PSP-derived intelligence in their counterterrorism efforts; the ODNI's support of the program by providing periodic threat assessments; and the DoJ's role in analyzing and certifying the legality of the PSP and managing use of PSP information in the judicial process.

(U) The IG reports also describe the conflicting views surrounding the legality of aspects of the PSP during 2003 and 2004, the confrontation between officials from DoJ and the White House about the legal basis for parts of the program and the resolution of that conflict. The ensuing transition of the PSP, in stages, from presidential authority to statutory authority under FISA, is also described in the IG reports.

(U) The IGs also examined the impact of PSP information on counterterrorism efforts. Many senior IC officials believe that the PSP filled a gap in intelligence collection thought to exist under FISA by increasing access to international communications that transited domestic U.S. communication wires, particularly international communications that originated or terminated within the United States. Others within the IC Community, including FBI agents, CIA analysts and managers, and other officials had difficulty evaluating the precise contribution of the PSP to counterterrorism efforts because it was most often viewed as one source among many available analytic and intelligence-gathering tools in these efforts. The IG reports describe several examples of how PSP-derived information factored into specific investigations and operations.

(U) The collection activities pursued under the PSP, and under FISA following the activities' transition to operation under that authority, as described in this report, resulted in unprecedented collection of communications content and metadata. We believe the retention and use by IC organizations of information collected under the PSP and FISA, particularly information on U.S. persons, should be carefully monitored.

This page intentionally left blank.

APPROVED FOR PUBLIC RELEASE

APPROVED FOR PUBLIC RELEASE

PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

(U) REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

REPORT NO. 2009-0013-AS

VOLUME I

(U) ANNEX TO THE REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

VOLUME II

10 JULY 2009

PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Special Warning

The report contains compartmented, classified material and no secondary distribution may be made without prior consent of the participating Inspectors General. Improper disclosure of this report may result in criminal, civil, or administrative penalties.

REPORT NO. 2009-0013-A

APPROVED FOR PUBLIC RELEASE

(U) Table of Contents

(U) The Deparment of Defense Inspector General's Review of the President's Surveillance Program 1

~~(S//NF)~~ The Central Intelligence Agency Inspector General's Review of CIA Participation in the President's Surveillance Program 11

(U) The National Security Agency, Central Security Service Inspector General's Review of the President's Surveillance Program 45

~~(S//NF)~~ The Office of the Director of National Intelligence Inspector General's Review of the Participation of the ODNI in the President's Surveillance Program 213

This page intentionally left blank.

APPROVED FOR PUBLIC RELEASE

~~TOP SECRET//STLW//SI//ORCON//NOFORN~~
~~SPECIAL ACCESS REQUIRED~~

Report No. 09-INTEL-08
June 26, 2009
Review

Inspector General
United States Department of Defense

DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

Review of the President's Surveillance Program (U)

~~Derived From: Multiple Sources~~
~~Declassify On: 20540511*~~

Copy____of____

~~TOP SECRET//STLW//SI//ORCON//NOFORN~~
~~SPECIAL ACCESS REQUIRED~~

This page intentionally left blank.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

June 26, 2009

MEMORANDUM FOR SECRETARY OF DEFENSE

SUBJECT: (U) Report on Review of the President's Surveillance Program Report No.: 09-INTEL-08 (U)

(U) We are providing this report for your information. This report fulfills the DoD Inspector General's requirement pursuant to Section 301 of Public Law 110-261, the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 (the Act). This report, along with reports prepared by the Inspectors General of the Department of Justice (DoJ), the Office of the Director of National Intelligence (DNI), Central Intelligence Agency (CIA), the National Security Agency (NSA), will be summarized in a comprehensive report as required by the Act.

~~(TS//STLW//SI//OC//NF)~~ **Results.** The OSD role in the establishment and implementation of the PSP was limited, with the burden of program execution residing with the NSA. We determined that there were six OSD officials with access to the PSP. These individuals had limited involvement, and did not make any additional tasking decisions beyond those directed for NSA implementation. We are aware of no other OSD involvement in the PSP.

(U) Background. The Act requires the IGs of the DoJ, DNI, NSA, the DoD, and any other element of the intelligence community that participated in the President's Surveillance Program (PSP)[1], to complete a comprehensive review of, with respect to the oversight authority and responsibility of each such IG:

- All facts necessary to describe establishment, implementation, product and use of the product in the program
- Access to legal reviews and access to information about the Program
- Communications and participation of individuals/entities related to the Program

[1] (U) The President's Surveillance Program is defined in the Act as the intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005 (commonly known as the Terrorist Surveillance Program).

~~Derived from: Multiple Sources~~
~~Declassify on: 20340511*~~

- Interaction with the Foreign Intelligence Surveillance Court and
- Any other matters identified by the IGs

~~(TS//STLW//SI//OC//NF)~~ **Scope and Methodology.** We conducted this review to examine the involvement of the Office of the Secretary of Defense (OSD), Department of Defense (DoD), in the establishment and implementation of the President's Surveillance Program (PSP). We interviewed current and former officials within OSD that had access to the PSP. We withdrew our request to interview Secretary of Defense Gates because he was provided access to the PSP after the program ended. The former Deputy Secretary of Defense Dr. Wolfowitz declined our request for an interview. We reviewed all relevant documentation within OSD and NSA related to OSD's involvement in the PSP. We also reviewed documentation at DoJ related to the PSP.

(U) The IGs of the DoJ, DoD, DNI, NSA, and CIA issued an interim report on September 10, 2008. In the interim report, the DoD IG stated that he would examine the involvement of the Office of the Secretary of Defense (OSD) in the establishment and implementation of the PSP. The NSA, as an agency within DoD performed the requirements of the PSP. As such, the NSA IG is conducting a review of NSA involvement with the PSP separate from this memorandum report.

~~(TS//STLW//SI//OC//NF)~~ **Implementation and Establishment of the PSP.** The OSD access to the PSP was limited to six individuals.[2] Those individuals are Secretary of Defense Robert Gates; former Secretary of Defense Donald Rumsfeld; former Deputy Secretary of Defense Paul Wolfowitz; Under Secretary of Defense for Intelligence (USD(I)) James Clapper[3]; former USD(I) Stephen Cambone; and Principal Deputy General Counsel Daniel Dell 'Orto.

~~(TS//STLW//SI//OC//NF)~~ The PSP was an extremely sensitive counterterrorism program focused on detecting and preventing terrorist attacks within the United States. The PSP was authorized by the President every 30 to 45 days and was initially directed against international terrorism; after March 2004, the PSP focused specifically against al-Qaeda and its affiliates. The Director of Central Intelligence (DCI), and later the DNI, would prepare a Threat Assessment

[2] ~~(TS//STLW//SI//OC//NF)~~ [redacted]

[3] ~~(TS//STLW//SI//OC//NF)~~ Secretary Gates and Under Secretary Clapper were provided access to the PSP after the PSP was transferred to Foreign Intelligence Surveillance Court supervision.

Memorandum, which validated the current threat to the United States. The Secretary of Defense would review and sign the Threat Assessment Memorandum. On three occasions, Dr. Wolfowitz, the former Deputy Secretary of Defense, signed the Threat Assessment Memoranda in the Secretary's absence. On two occasions, Dr. Cambone, the former USD(I), signed the Threat Assessment Memoranda when Secretary Rumsfeld and Dr. Wolfowitz were unavailable.

~~(TS//STLW//SI//OC//NF)~~ Once the Threat Assessment Memorandum was signed, the President would then sign a Presidential Authorization with the Threat Memorandum attached. The President would task the Secretary of Defense to employ DoD resources to execute the requirements set forth in the Presidential Authorization. The Attorney General, or his designee, would certify the Presidential Authorization for form and legality. The Secretary of Defense would then direct the actions authorized by the Presidential Authorization to the NSA for implementation. On one occasion, Dr. Wolfowitz, the former Deputy Secretary of Defense, directed the Director of NSA to implement the Presidential Authorization, in the Secretary's absence. On a separate occasion, Dr. Cambone, the former USD(I), directed the Director of NSA to implement the Presidential Authorization.

~~(TS//SI//NF)~~ **Interaction with the Foreign Intelligence Surveillance Court.** Dr. Wolfowitz also executed two declarations to the U.S. Foreign Intelligence Surveillance Court. The first, executed on [redacted] was in support of the Government's Application seeking renewal, in part, of the authority to install and use pen register and trap and trace devices, in order to obtain information [redacted] pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. sections 1801-1811, 1841-1846, as amended. The initial authority under FISA to install and use pen register and trap and trace devices for that purpose was granted by the Foreign Intelligence Surveillance Court on July 14, 2004, [redacted]

~~(TS//SI//NF)~~ Dr. Wolfowitz's second declaration was executed on [redacted] That declaration was made in response to the Foreign Intelligence Surveillance Court's [redacted] Order requiring the Government to submit a declaration from the Deputy Secretary of Defense discussing NSA' violations of the Court's July 14 Order authorizing NSA to install and use pen register and trap and trace devices in order to obtain information about [redacted] In that declaration, Dr. Wolfowitz stated the circumstances surrounding unauthorized collection that occurred, the disposition of information collected without authorization, steps NSA took to remedy the violation, and measures NSA implemented to prevent recurrence of such violations.

APPROVED FOR PUBLIC RELEASE

~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~

(U) Should you have questions on this request, please feel free to contact me, [illegible] at (703) 61[illegible].

APPENDIX (U)

REPORT DISTRIBUTION LIST (U)

(U)

OFFICE OF THE SECRETARY OF DEFENSE

Secretary of Defense
Under Secretary of Defense for Intelligence
Deputy General Counsel, Intelligence

OTHER DEFENSE ORGANIZATION

Inspector General, National Security Agency

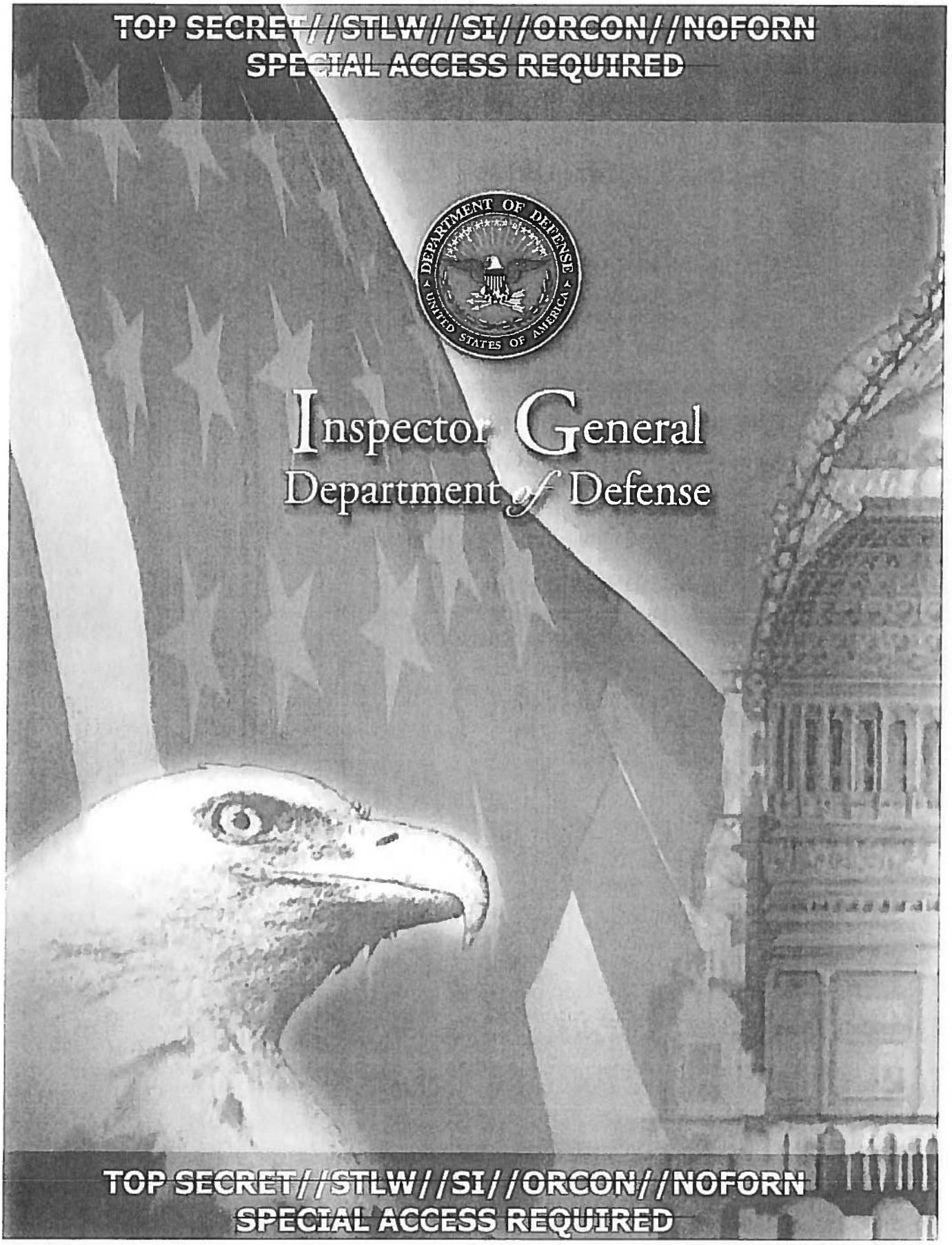
NON-DEFENSE FEDERAL ORGANIZATIONS

Inspector General, Director of National Intelligence
Inspector General, Department of Justice
Inspector General, Central Intelligence Agency

CONGRESSIONAL COMMITTEES

Senate Judiciary Committee
Senate Select Committee on Intelligence
House Judiciary Committee
House Permanent Select Committee on Intelligence

APPROVED FOR PUBLIC RELEASE



This page intentionally left blank.

This page intentionally left blank.

APPROVED FOR PUBLIC RELEASE

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

CENTRAL INTELLIGENCE AGENCY

Office of Inspector General

(U) FINAL REPORT

~~(S//NF)~~ CIA Participation in the President's Surveillance Program

Report No. 2008-0016-AS

[redacted]

30 June 2009

Issue Date

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

This page intentionally left blank.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

(U) Table of Contents

(U) EXECUTIVE SUMMARY 1

(U) BACKGROUND 3

(U) Origin and Scope of the Review 4

(U) The President's Surveillance Program 5

(U) REVIEW RESULTS 6

~~(S//NF)~~ CIA Participation in the President's Surveillance Program 6

~~(TS//STLW//SI//OC/NF)~~ CIA Prepared the Threat Assessment Memorandums Supporting Authorization of the President's Surveillance Program 7

(U//~~FOUO~~) CIA Tasked and Received Reporting From the President's Surveillance Program 9

(U//~~FOUO~~) Procedures and Standards for Requesting Information 9

(U//~~FOUO~~) Reporting Provided in Response to Requests for Information 10

(U//~~FOUO~~) Primary CIA Users of the President's Surveillance Program 11

(U//~~FOUO~~) CIA Requests for Information Were Adequately Justified 13

(U//~~FOUO~~) Senior CIA Officials Believe That the President's Surveillance Program Filled an Intelligence Gap 13

(U//~~FOUO~~) The CIA Did Not Assess the Effectiveness of the President's Surveillance Program 15

(U) Counterterrorism Successes Supported by the President's Surveillance Program 16

~~(S//NF)~~ Several Factors Hindered CIA Utilization of the President's Surveillance Program 17

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

(U) CIA Had Limited Access to Legal Reviews of the President's Surveillance Program 19

~~(S//NF)~~ CIA Officials Sought to Delay Exposure of the President's Surveillance Program by the *New York Times* 20

(U) Methodology ..... Exhibit A

(U) Threat Assessment Memorandum Concluding Paragraph ..... Exhibit B

(U) Example of Link Diagram From August 2002 ..... Exhibit C

(U) Review Team ..... Exhibit D

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~(S//NF)~~ CIA Participation in the President's Surveillance Program

(U) EXECUTIVE SUMMARY

~~(S//NF)~~ Title III of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 requires the Inspectors General (IGs) of the elements of the Intelligence Community (IC) that participated in the President's Surveillance Program (PSP) to conduct a comprehensive review of the program. The results of our review of CIA participation in the PSP are presented in this report, and will be included in the comprehensive report required to be provided to the appropriate committees of Congress by 10 July 2009.

~~(TS//STLW//SI//OC/NF)~~ The CIA prepared the threat assessment memorandums that were used to support Presidential authorization and periodic reauthorizations of the PSP. The threat assessment memorandums were prepared by personnel from the CIA [redacted] Each of the memorandums focused on the current threat situation and did not provide an assessment of the PSP's utility in addressing previously reported threats. The threat assessment memorandums were signed by the Director of Central Intelligence (DCI) and forwarded to the Secretary of Defense to be co-signed. Responsibility for drafting the threat assessment memorandums was transferred to the newly-established Terrorist Threat Integration Center in May 2003 and retained by TTIC's successor organization, NCTC (the National Counterterrorism Center). The DCI continued to sign the threat assessment memorandums through 15 April 2005. Subsequent memorandums were signed by the Director of National Intelligence.

~~(TS//STLW//SI//OC/NF)~~ CIA analysts and targeters, as PSP consumers, tasked the program and utilized the product from the program in their analyses.

[redacted]

1

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

[redacted]

~~(TS//STLW//SI//OC/NF)~~ Two former Directors, a former Acting Director, and other senior CIA officials we interviewed told us that the PSP addressed a gap in intelligence collection. [redacted] However, collection of such communications required authorization under FISA, and there was widespread belief among senior IC and CIA officials that the process for obtaining FISA authorization was too cumbersome and time consuming to address the current threat. Current and former CIA officials emphasized the increased timeliness, flexibility, and access provided by the PSP as compared to the process for obtaining a warrant under FISA.

~~(TS//STLW//SI//OC/NF)~~ The CIA did not implement procedures to assess the usefulness of the product of the PSP and did not routinely document whether particular PSP reporting had contributed to successful counterterrorism operations. CIA officials told us that PSP reporting was used in conjunction with reporting from other intelligence sources and was rarely the sole basis for a counterterrorism success. [redacted] CIA officers, even those read into the program, would have been unaware of the full extent of PSP reporting. Consequently, there is no means to comprehensively track how PSP information was used. CIA officials were able to provide only limited information on how program reporting contributed to successful operations, and therefore, we were unable to independently draw any conclusion on the overall usefulness of the program to CIA.

~~(S//NF)~~ Several factors hindered the CIA in making full use of the capabilities of the PSP. Many CIA officials told us that too few CIA personnel at the working level were read into the PSP. [redacted] officials told us that CIA analysts and targeting officers who were read in had too many competing priorities and too many other available information sources and analytic tools—many of which were more easily accessed and timely—to fully utilize the PSP. CIA officers also told us that the PSP would have been more fully utilized if analysts and targeting officers had obtained a better understanding of the program's capabilities. Many CIA officers noted that there was insufficient training and legal guidance concerning the program's capabilities and the use of PSP-derived information. The factors that hindered the CIA in making full use of the PSP might have been mitigated if the CIA had designated an individual at an appropriate level of managerial authority, who possessed knowledge of both the PSP and CIA counterterrorism activities, to be responsible and accountable for overseeing CIA participation in the program.

~~(TS//STLW//SI//OC/NF)~~ There is no indication that personnel from the CIA Office of General Counsel or other CIA components were involved in preparing the legal memorandums supporting the PSP that were produced by the Department of Justice, Office of Legal Counsel (OLC). CIA OGC personnel had very limited access to these memorandums.

~~(S//NF)~~ Senior CIA officials participated in meetings with a *New York Times* editor and reporter and senior Administration officials concerning an article the newspaper was preparing concerning the PSP.

[redacted]
Assistant Inspector General for Audit

This page intentionally left blank.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

(U) BACKGROUND

(U) Origin and Scope of the Review

(U) Title III of the Foreign Intelligence Surveillance Act Amendments Act of 2008, which was signed into law on 10 July 2008, requires the IGs of the elements of the Intelligence Community that participated in the PSP to conduct a comprehensive review of the program.[1] The review required to be conducted under the Act is to examine:

> (A) all of the facts necessary to describe the establishment, implementation, product, and use of the product of the Program;
>
> (B) access to legal reviews of the program and access to information about the Program;
>
> (C) communications with, and participation of, individuals and entities in the private sector related to the Program;
>
> (D) interaction with the Foreign Intelligence Surveillance Court and transition to court orders related to the Program; and
>
> (E) any other matters identified by any such Inspector General that would enable that Inspector General to complete a review of the Program, with respect to such Department or element.

~~(TS//STLW//SI//OC/NF)~~ The interim report required under the Act was submitted to the committees of Congress prescribed in the Act on 10 September 2008. That report described the scope of the work to be conducted by each of the participating IGs, which include the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and the CIA. Our review of CIA participation in the PSP examined CIA's :

- Role in preparing the threat assessments and legal certifications supporting periodic reauthorization of the PSP.
- Role in identifying targets for the PSP.

---

[1] ~~(S//NF)~~ The President's Surveillance Program is defined in the Act as the intelligence activity involving communications that was authorized by the President during the period beginning on 11 September 2001, and ending on 17 January 2007, including the program referred to by the President in a radio address on 17 December 2005 (commonly known as the Terrorist Surveillance Program). The classified name for the President's Surveillance Program is "STELLARWIND."

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

[redacted]

The results of our review of CIA participation in the PSP are presented in this report, and will be included in the comprehensive final report required to be provided to the appropriate committees of Congress by 10 July 2009.

(U) The President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ According to former Director of the NSA and former Director of the CIA (DCIA) Michael V. Hayden, initial discussions concerning the activities that would become the PSP occurred less than two weeks after the 11 September 2001 terrorist attacks in a meeting between DCI George J. Tenet and Vice President Richard B. Cheney. Although Hayden did not attend the meeting, he was told by Tenet that Cheney asked if the Intelligence Community was doing everything possible to prevent another terrorist attack. In response, Tenet described [redacted] Cheney then asked if there was more that NSA could do. This led to discussions between Cheney, Hayden, Cheney's legal counsel David S. Addington, and senior NSA officials. It was determined that the NSA had the capability to collect additional wire communications that could enhance the IC's counterterrorism efforts, but that new authority was needed to employ the capability. The determination led to the authorization of the PSP by President George W. Bush on 4 October 2001.

~~(TS//STLW//SI//OC/NF)~~ The PSP was intended to help prevent additional terrorist attacks against the US Homeland. Although the authorized collection activities changed over the life of the program, in general, the program authorized the NSA to acquire content and/or metadata concerning telephone and e-mail communications for which there were reasonable grounds to believe that at least one of the participants in the communication was located outside the US and that a party to

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

the communication was affiliated with a group engaged in international terrorism. The collection activities conducted under the PSP were brought under Foreign Intelligence Surveillance Court oversight in stages between July 2004 and January 2007.[2]

~~(TS//STLW//SI//OC/NF)~~ Under the PSP, the NSA collected three sets of data. The first set included the content of individually targeted telephone and e-mail communications. The second set consisted of telephone dialing information—the date, time, and duration of calls; the telephone number of the caller; and the number receiving the call—collected in bulk [redacted] The third data set consisted of e-mail transactional data— [redacted] collected in bulk [redacted]

(U) REVIEW RESULTS

~~(S//NF)~~ CIA Participation in the President's Surveillance Program

[redacted]

[2] (U) The Foreign Intelligence Surveillance Act of 1978 established the Foreign Intelligence Surveillance Court to oversee requests for surveillance warrants by federal agencies against suspected foreign intelligence agents inside the US.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

[redacted]

~~(TS//STLW//SI//OC/NF)~~ [redacted] CIA personnel prepared the threat assessment memorandums that were used to support the initial Presidential authorization and subsequent reauthorizations of the PSP. [redacted]

~~(TS//STLW//SI//OC/NF)~~ CIA Prepared the Threat Assessment Memorandums Supporting Authorization of the President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ The CIA initially prepared the threat assessment memorandums that were used to support Presidential authorization and periodic reauthorizations of the PSP. The memorandums documented the current threat to the US homeland and to US interests abroad from al-Qa'ida and affiliated terrorist organizations. The first threat assessment memorandum—*The Continuing Near-Term Threat from Usama Bin Ladin*—was signed by DCI Tenet on 4 October 2001.[3] Subsequent threat assessment memorandums were prepared every 30 to 60 days to correspond with the President's reauthorizations of the PSP.

~~(TS//STLW//SI//OC/NF)~~ The DCI Chief of Staff, John H. Moseman, was the CIA focal point for preparing the threat assessment memorandums. According to Moseman, he directed the [redacted] to prepare objective appraisals of the current terrorist threat, focusing primarily on threats to the homeland, and to document those appraisals in a memorandum. Initially, the [redacted] analysts who prepared the threat assessments were not read into the PSP and did not know how the threat assessments would be used. [redacted] analysts drew upon all sources of intelligence in preparing their threat assessments. Each of the memorandums focused on the current threat situation and did not provide an assessment of the PSP's utility in addressing previously reported threats.

---

[3] ~~(S//NF)~~ The title of the threat assessment memorandums was changed to *The Global War Against Terrorism* in June 2002.

~~TOP SECRET//STLW//HCS//COMINT//ORCON//NOFORN~~

~~(TS//STLW//SI//OC/NF)~~ After [redacted] completed its portion of the memorandums, the DCI's Chief of Staff added a paragraph at the end of the memorandums stating that the individuals and organizations involved in global terrorism (and discussed in the memorandums) possessed the capability and intention to undertake further terrorist attacks within the US. Moseman recalled that the paragraph was provided to him initially by either White House Counsel Alberto R. Gonzales or Addington. The paragraph recommended that the President authorize the Secretary of Defense to employ within the US the capabilities of the Department of Defense, including but not limited to NSA's signals intelligence capabilities, to collect foreign intelligence by electronic surveillance. The paragraph also described the types of communication and data that would be collected and the circumstances under which they could be collected.[4] The draft threat assessment memorandums were then reviewed by Office of General Counsel attorneys assigned to [redacted] and Acting General Counsel (Senior Deputy General Counsel) John A. Rizzo. Rizzo told us that the draft memorandums were generally sufficient, but that there were occasions when, based on his experience with previous memorandums, he thought that draft memorandums contained insufficient threat information or did not present a compelling case for reauthorization of the PSP. In such instances, Rizzo would request tha[redacted] provide additional available threat information or make revisions to the draft memorandums.

~~(TS//STLW//SI//OC/NF)~~ The threat assessment memorandums were then signed by DCI Tenet and forwarded to the Secretary of Defense to be co-signed. Tenet signed most of the threat memorandums prepared during his tenure as DCI. On the few occasions when he was unavailable, the Deputy Director of Central Intelligence (DDCI), John E. McLaughlin, signed the memorandums on behalf of Tenet. McLaughlin also signed the memorandums in the capacity of Acting DCI in August and September 2004. In November 2004, Porter J. Goss became DCI and assumed responsibility for signing the memorandums. There were no occasions when the DCI or Acting DCI withheld his signature from the threat assessment memorandum. After they were signed by the Secretary of Defense, the memorandums were reviewed by the Attorney General and delivered to the White House to be attached to the PSP reauthorization memorandums signed by the President.

~~(TS//STLW//SI//OC/NF)~~ Responsibility for drafting the threat assessment memorandums was transferred from [redacted] to the newly established Terrorist Threat Integration Center in May 2003. This responsibility was retained by TTIC's successor organization, NCTC. The DCI continued to sign the threat assessment memorandums

---

[4] (U) Exhibit B presents the conclusion and recommendation paragraph included in the threat assessment memorandum dated 10 January 2005. Similar language was included in each of the memorandums.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

through 15 April 2005. Subsequent memorandums were signed by the Director of National Intelligence.[5]

(U//~~FOUO~~) CIA Tasked and Received Reporting From the President's Surveillance Program

(U//~~FOUO~~) Procedures and Standards for Requesting Information

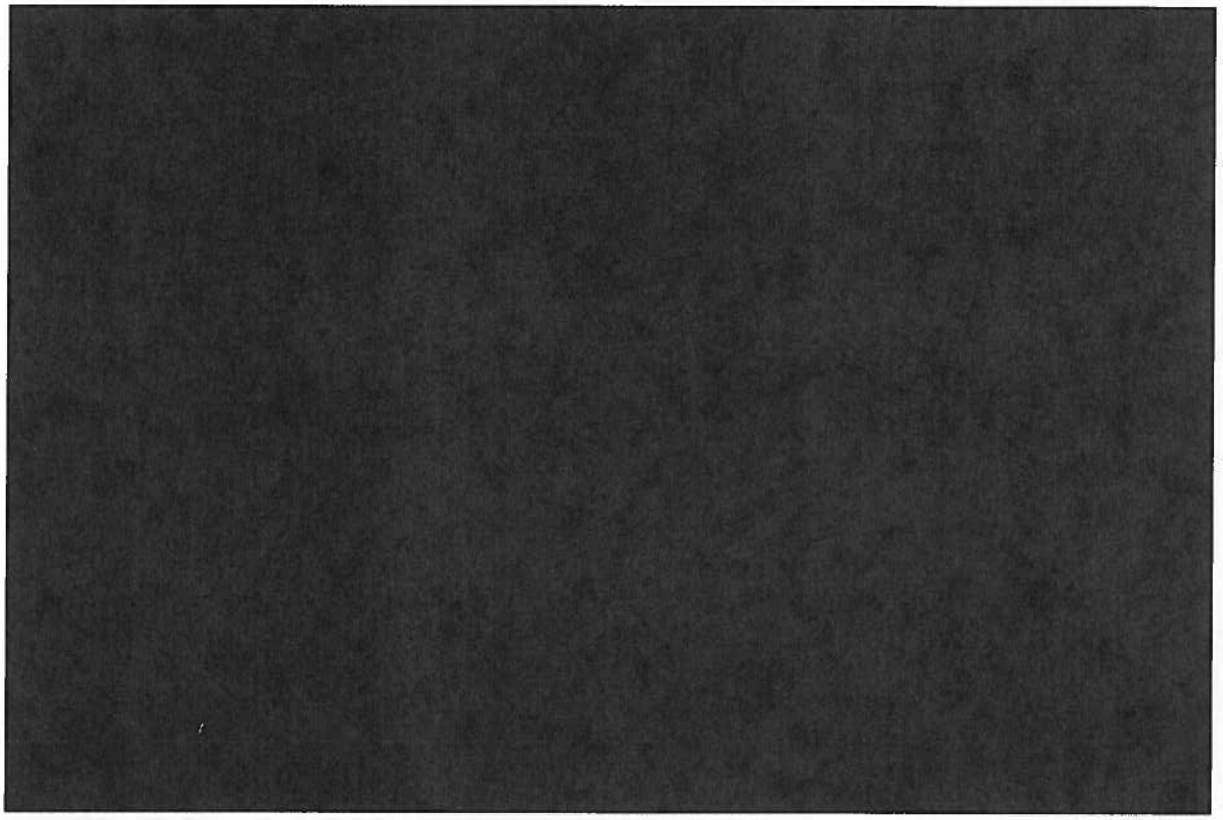
[redacted]

9

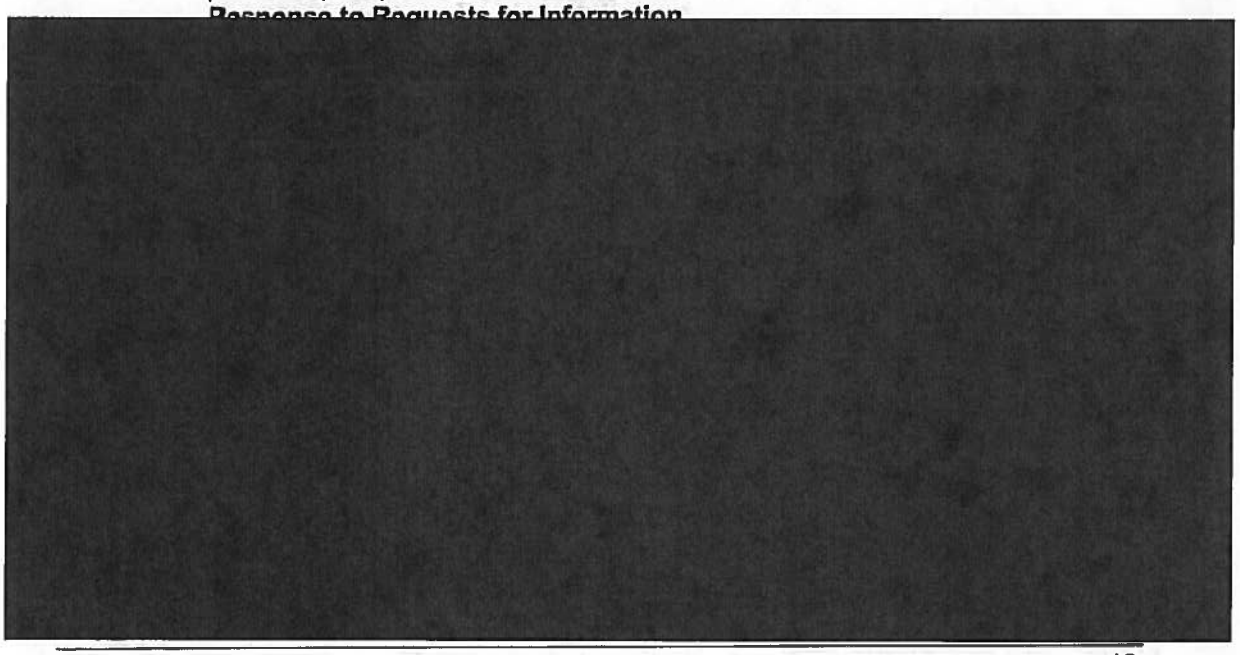
~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

APPROVED FOR PUBLIC RELEASE

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~



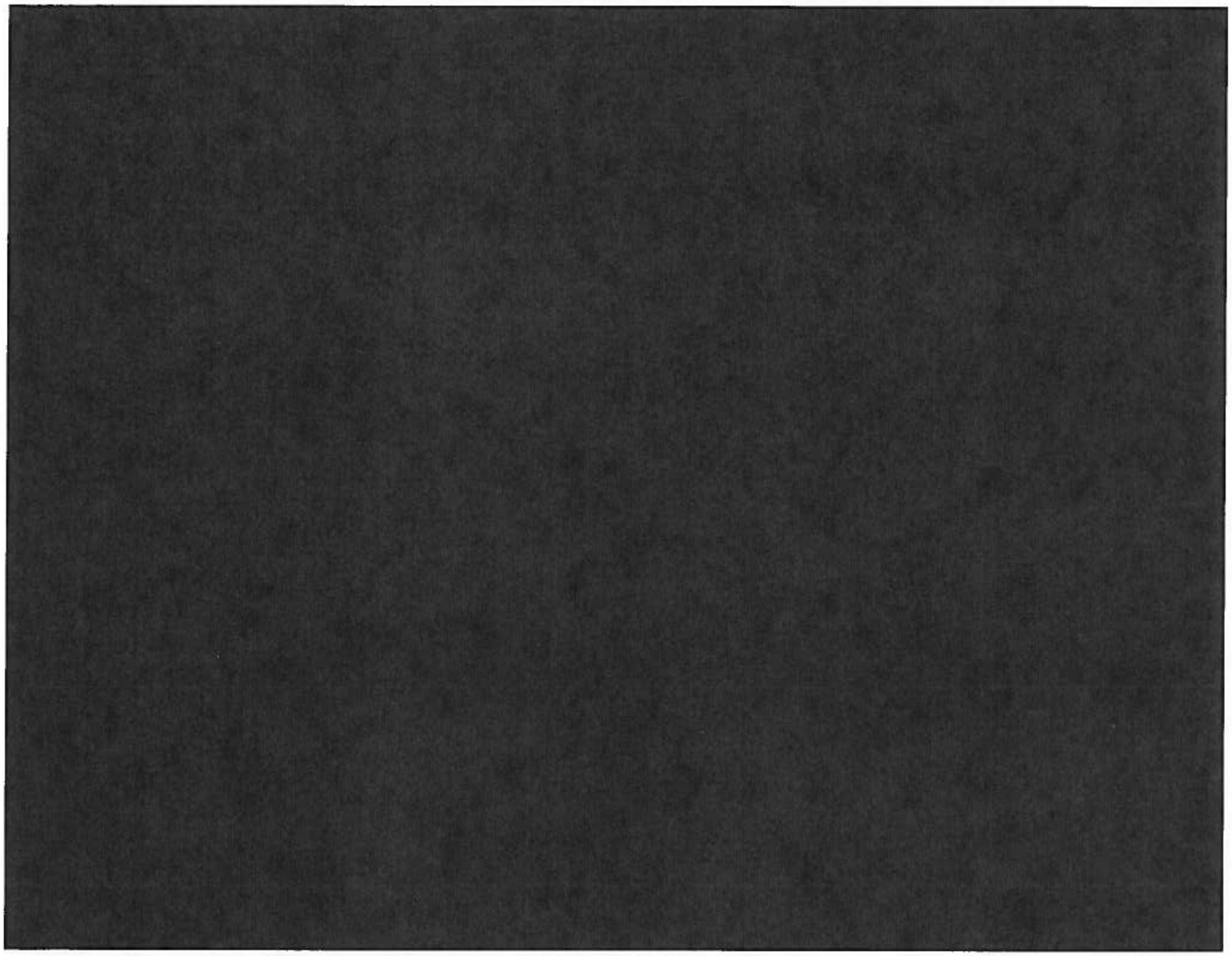
(U//~~FOUO~~) Reporting Provided in
Response to Requests for Information



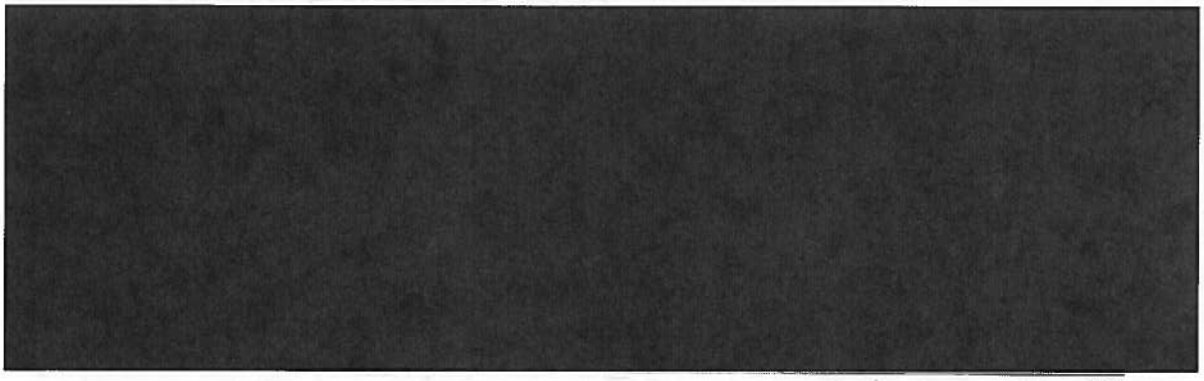
~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~



(U//~~FOUO~~) Primary CIA Users of the President's Surveillance Program

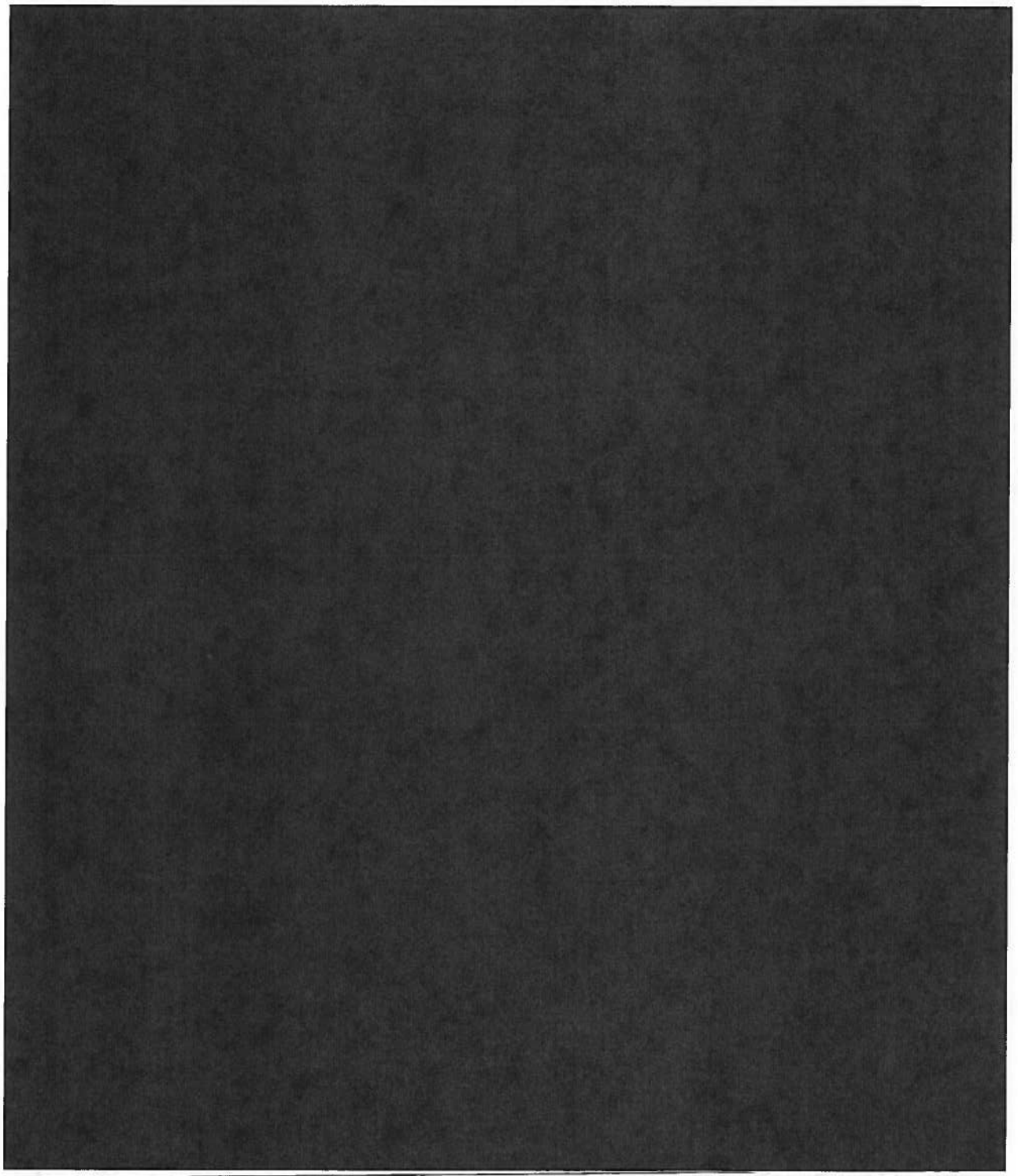


11

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

APPROVED FOR PUBLIC RELEASE

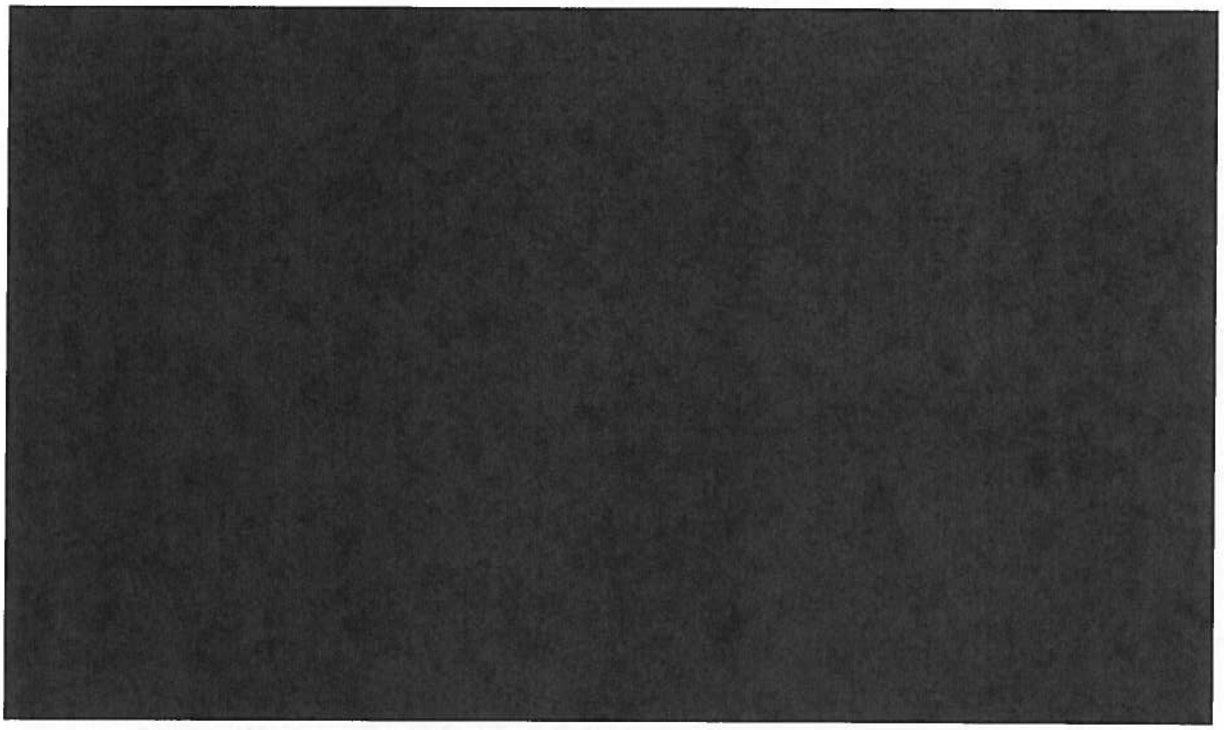
~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~



12

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~



(U//~~FOUO~~) Senior CIA Officials Believe That the President's Surveillance Program Filled an Intelligence Gap

~~(TS//STLW//SI//OC/NF)~~ Former Directors Hayden and Goss, former Acting Director McLaughlin, and other senior CIA officials we interviewed told us that the PSP addressed a gap in intelligence collection. Following the terrorist attacks on 11 September 2001, there was concern that additional acts of terrorism would be perpetrated by terrorist cells already inside the US. [redacted] However, collection of such communications required authorization under FISA, and there was widespread belief among senior IC and CIA officials that the process for obtaining FISA authorization was too cumbersome and time consuming to address the current threat.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

[redacted]

~~(TS//STLW//SI//OC/NF)~~ Other senior CIA officials told us that the PSP provided CIA access to information that was previously unavailable. [redacted]

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

(U//~~FOUO~~) The CIA Did Not Assess the Effectiveness of the President's Surveillance Program

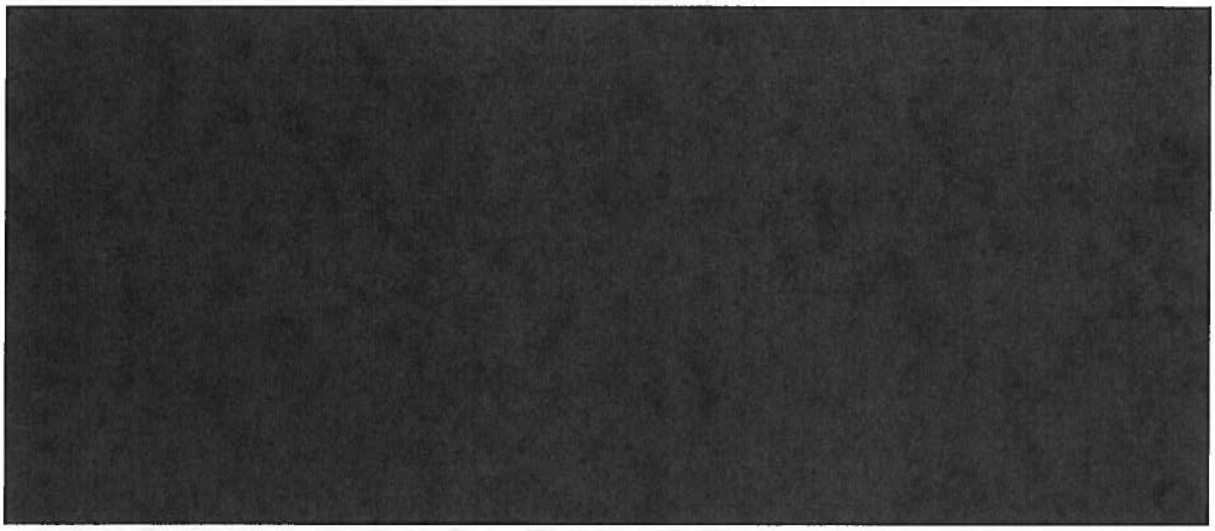
~~(TS//STLW//SI//OC/NF)~~ The CIA did not implement procedures to assess the usefulness of the product of the PSP and did not routinely document whether particular PSP reporting had contributed to successful counterterrorism operations. CIA officials, including DCIA Hayden, told us that PSP reporting was used in conjunction with reporting from other intelligence sources; consequently, it is difficult to attribute the success of particular counterterrorism operations exclusively to the PSP. In a May 2006 briefing to the Senate Select Committee on Intelligence (SSCI), the Deputy Director, [redacted] said that PSP reporting was rarely the sole basis for an intelligence success, but that it frequently played a supporting role. He went on to state that the program was an additional resource to enhance the CIA's understanding of terrorist networks and to help identify potential threats to the homeland. Other [redacted] officials we interviewed said that the PSP was one of many tools available to them, and that the tools were often used in combination.

[redacted]

15

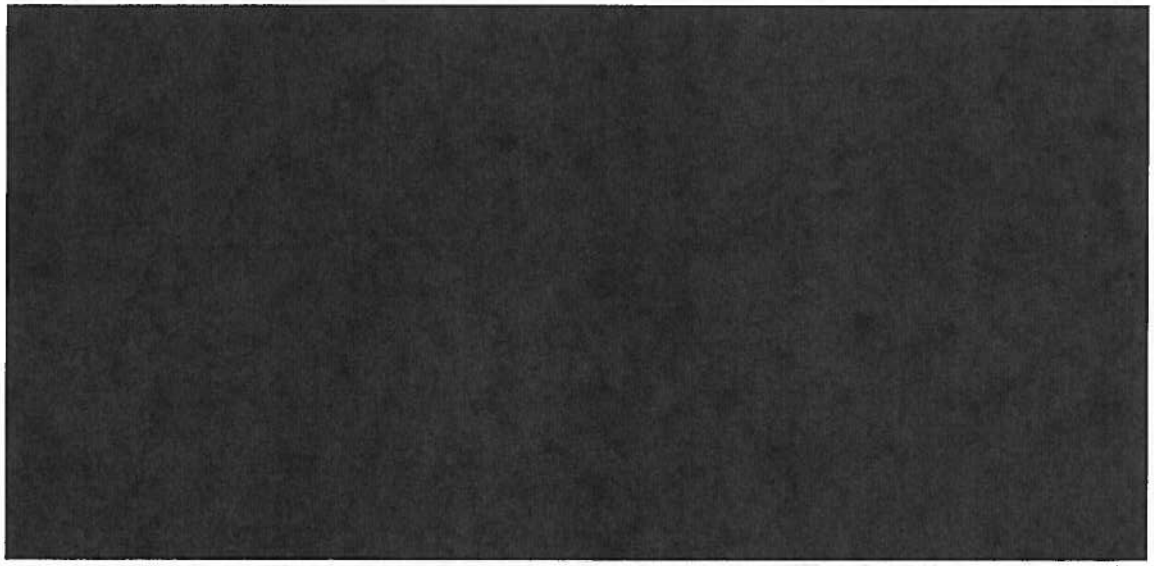
~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

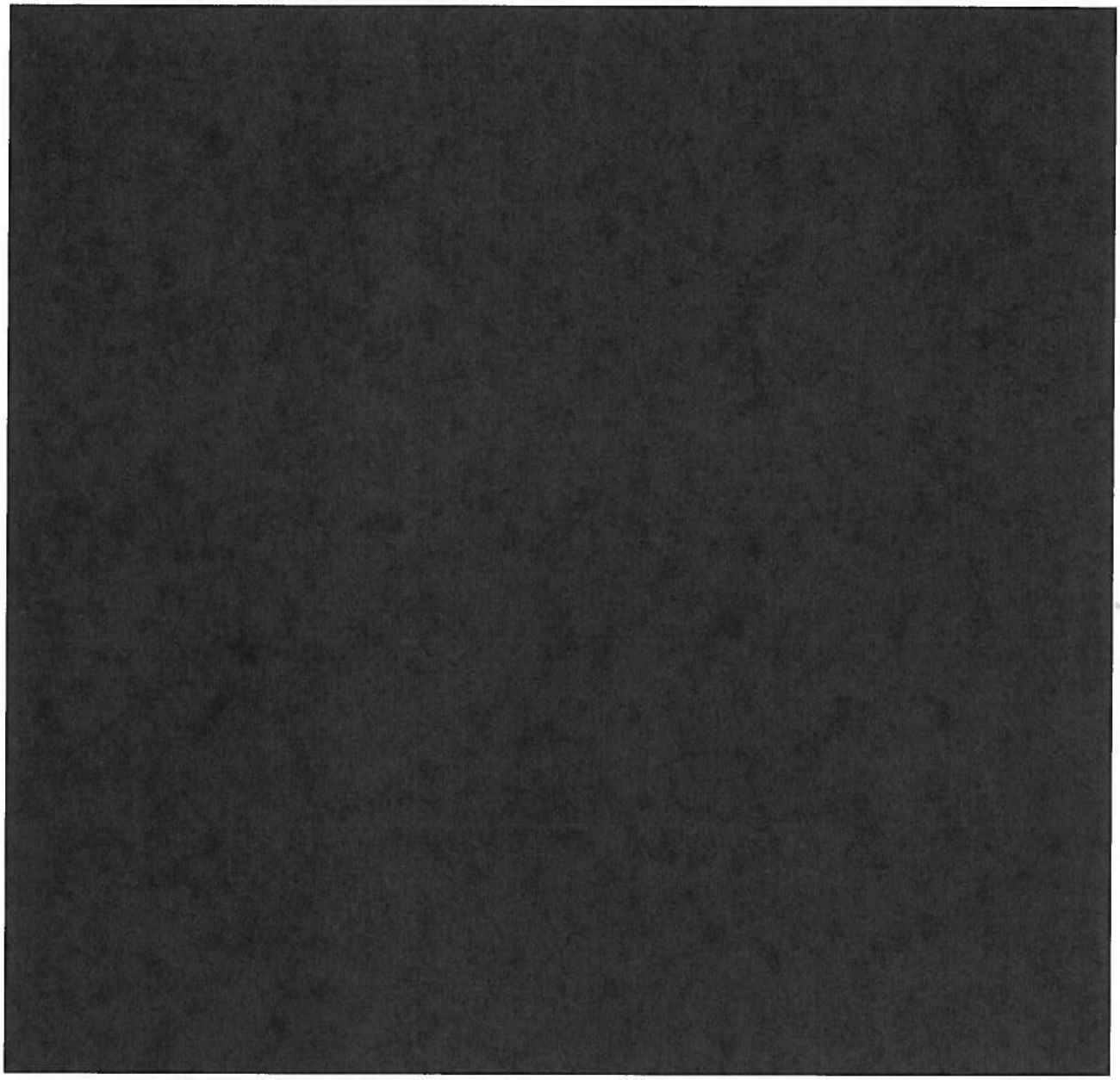


(U) Counterterrorism Successes Supported by the President's Surveillance Program

~~(S//NF)~~ Despite the fact that CIA officials we interviewed did not provide much specific information on PSP-derived counterterrorism successes, some key counterterrorism operations supported by the PSP were cited in briefings presented by CIA officials. In March 2004, the CIA provided a series of three briefings at the White House to senior Administration officials and Congressional leaders. These briefings included operational details concerning the PSP as well as examples of program successes. In May 2006, the Deputy Director, [redacted] briefed SSCI members and staff on the usefulness to [redacted] of the PSP.



~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~



~~(S//NF)~~ Several Factors Hindered CIA Utilization of the President's Surveillance Program

~~(S//NF)~~ Several factors hindered the CIA in making full use of the capabilities of the PSP. Many CIA officials told us that too few CIA personnel at the working level were read into the PSP. At the program's inception, a disproportionate number of the

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

CIA personnel who were read into the PSP were senior CIA managers, [redacted]

~~(S//NF)~~ [redacted] officials also told us that working-level CIA analysts and targeting officers who were read into the PSP had too many competing priorities, and too many other information sources and analytic tools available to them, to fully utilize PSP. [redacted] officials also told us that much of the PSP reporting was vague or without context, which led analysts and targeting officers to rely more heavily on other information sources and analytic tools, which were more easily accessed and timely than the PSP.

~~(S//NF)~~ CIA officers also told us that the PSP would have been more fully utilized if analysts and targeting officers had obtained a better understanding of the program's capabilities. There was no formal training on the use of the PSP beyond the initial read in to the program. Many CIA officers we interviewed said that the instruction provided in the read-in briefing was not sufficient and that they were surprised and frustrated by the lack of additional guidance. Some officers told us that there was insufficient legal guidance on the use of PSP-derived information. [redacted]

~~(S//NF)~~ The factors that hindered the CIA in making full use of the PSP might have been mitigated if the CIA had designated an individual at an appropriate level of managerial authority, who possessed knowledge of both the PSP and CIA counterterrorism activities, to be responsible and accountable for overseeing CIA participation in the program. [redacted]

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

[redacted]

(U) CIA Had Limited Access to Legal Reviews of the President's Surveillance Program

~~(TS//STLW//SI//OC/NF)~~ There is no indication that personnel from the CIA Office of General Counsel or other CIA components were involved in preparing the legal memorandums supporting the PSP that were produced by the Department of Justice, Office of Legal Counsel (OLC). At the time of the initial authorization of the PSP (4 October 2001), Robert M. McNamara, Jr. was the CIA General Counsel. There is no record that McNamara was ever read into PSP, and he retired from the CIA on 15 November 2001. Acting General Counsel John Rizzo was read into the program on 21 December 2001, but, at that time, he was not provided access to the OLC legal opinions. Rizzo told us that by working through Addington, with whom Rizzo was acquainted, he eventually was allowed to read the OLC legal memorandums at Addington's office in July 2004.

~~(TS//STLW//SI//OC/NF)~~ Scott W. Muller became the CIA General Counsel on 24 October 2002. Although NSA records do not indicate that Muller was read into PSP, during our interview with Muller, he acknowledged having been read into the program and having read the OLC legal memorandums supporting the program. After Jack L. Goldsmith became the Assistant Attorney General for the Office of Legal Counsel in October 2003, the OLC undertook a reassessment of the legal rationale for the PSP. Muller recounted discussions with Deputy Attorney General James B. Comey around March 2004 concerning the legal basis for certain aspects of the program. Muller told us that he shared Comey's concern [redacted] Several of the senior CIA managers we interviewed said that, although they were concerned that the PSP operate within legal authorities, they believed that it was important to continue CIA

participation in the program because CIA analysts and targeters had told them that the program was a useful counterterrorism tool.

~~(S//NF)~~ CIA Officials Sought to Delay Exposure of the President's Surveillance Program by the *New York Times*

~~(S//NF)~~ In October 2004, James Risen, a reporter for *The New York Times*, contacted the CIA Office of Public Affairs seeking an interview with DCI Goss concerning an article the newspaper was planning on the PSP. Senior officials from the CIA, NSA, Office of the Vice President, and the Office of the Secretary of Defense met to discuss a response. On 20 October 2004, DDCI McLaughlin and DCI Chief of Staff Moseman met with the Washington, DC editor of *The New York Times*, Philip Taubman, and Risen. According to a memorandum for the record prepared by Moseman, McLaughlin did not provide any details regarding the PSP or comment on the legal basis for the program, but he stressed that publication of the article would expose, and potentially compromise, effective counterterrorism tools.

~~(S//NF)~~ [redacted] Ultimately, based on assurances from Hayden that he would advise them of inquiries from other news organizations concerning the PSP, Taubman and Risen agreed to hold the article and publish it only when it became apparent that other news organizations were preparing their own stories on the PSP. On 16 December 2005, *The New York Times* published its first article on the PSP: "Bush Lets U.S. Spy on Callers Without Courts." On 17 December 2005, President Bush publicly confirmed in a radio address the existence of the disclosed portion of the PSP.

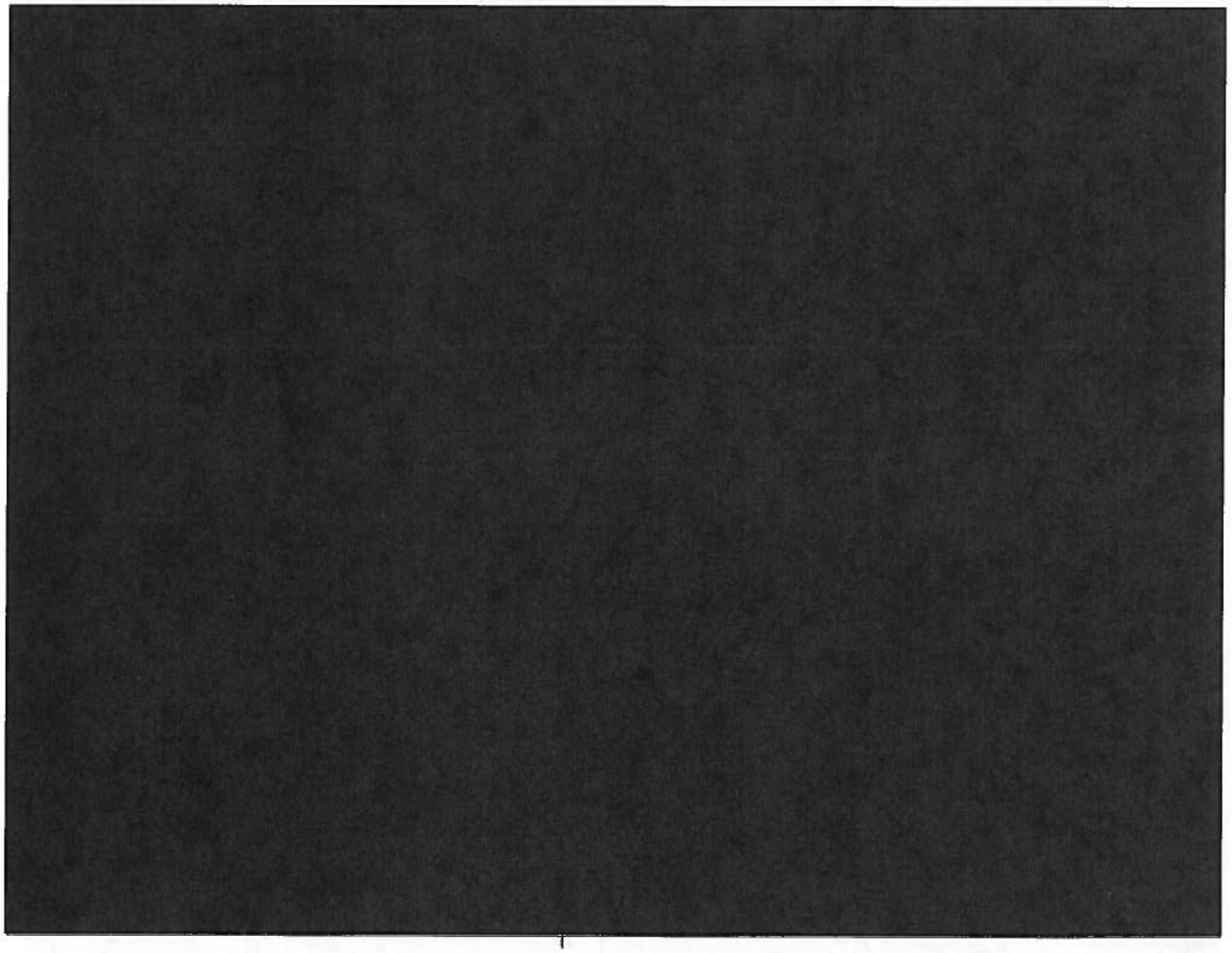
This page intentionally left blank.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

Exhibit A

(U) Methodology

(U//~~FOUO~~) During our review, we conducted 50 interviews of current and former CIA personnel who had been involved with the President's Surveillance Program (PSP). Among the senior CIA officials we interviewed were former Director of the National Security Agency (NSA) and former Director of the CIA (DCIA) Michael V. Hayden, former Director of Central Intelligence (DCI) and former DCIA Porter J. Goss, and former Acting DCI John E. McLaughlin. We contacted former DCI George J. Tenet for an interview. Tenet suggested that we first interview his former Chief of Staff, John H. Moseman, and then contact him if we still had a need to interview him. Following our interview with Moseman, we contacted Tenet's office several times to request an interview, but he did not return our telephone calls.



~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

[redacted]

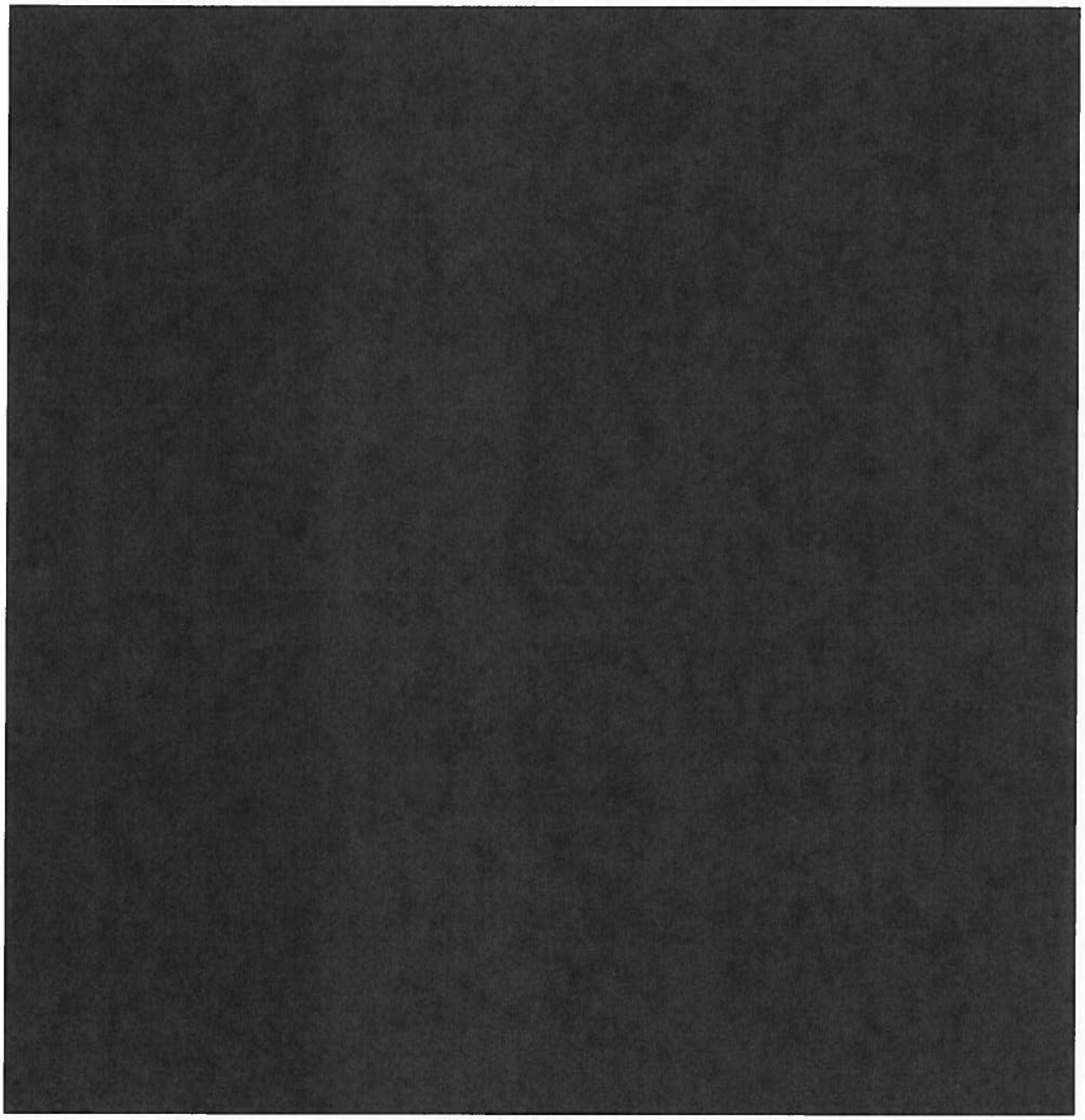
(U//~~FOUO~~) Management comments were received from Michael V. Hayden; Scott W. Muller; John H. Moseman; the Director, [redacted] and the Chief [redacted] Their comments were considered in preparation of the final report.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

Exhibit B

(U) Threat Assessment Memorandum Concluding Paragraph

[Excerpt from the *Global War Against Terrorism* memorandum dated 10 January 2005.]

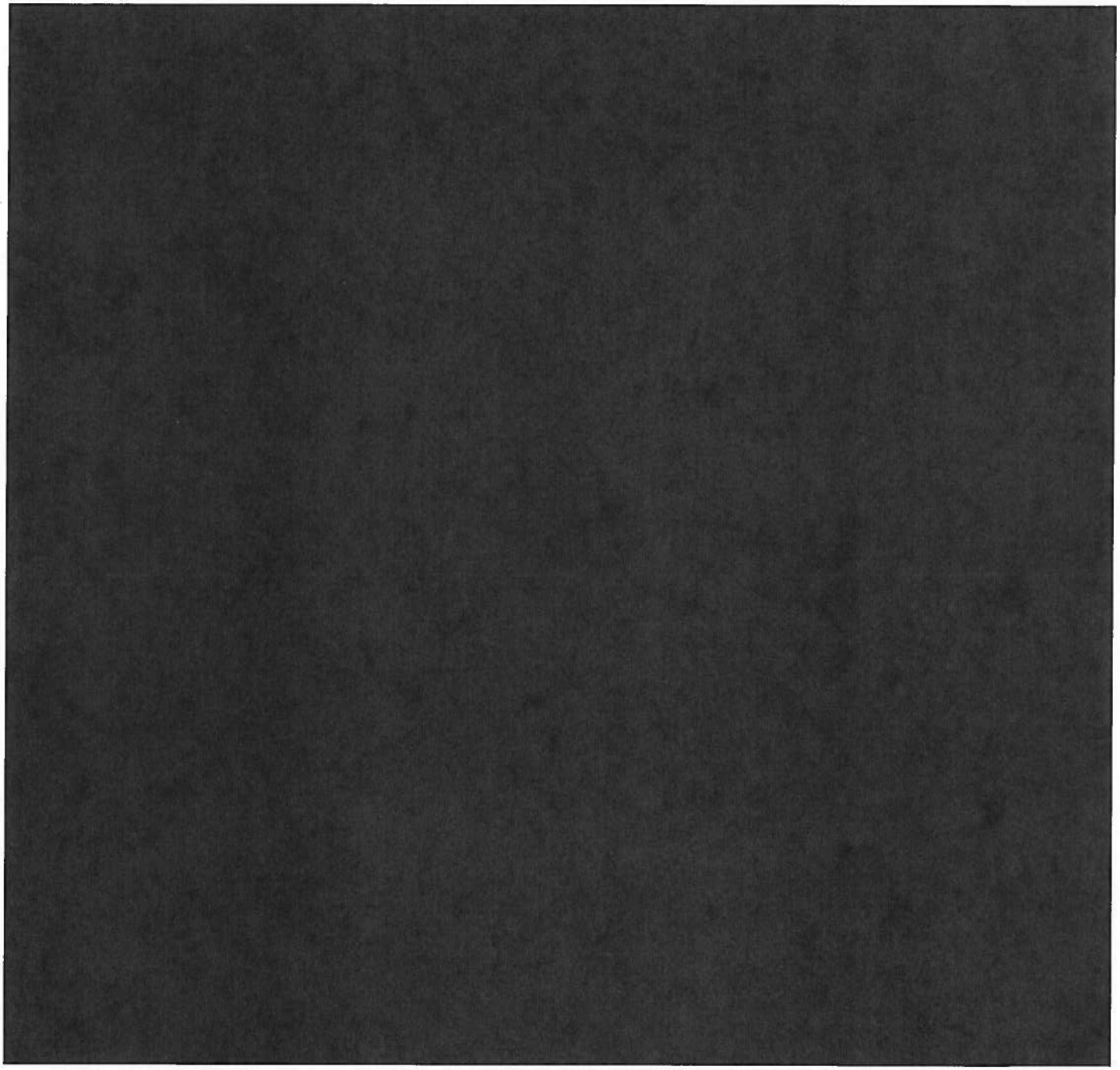


~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

This page intentionally left blank.

Exhibit C

(U) Example of a Link Diagram From August 2002



This page intentionally left blank.

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

Exhibit D

(U) Review Team

(U//~~FOUO~~) This report was prepared by the Operations Division, Audit Staff, Office of Inspector General.

[redacted] Division Chief
[redacted] Project Manager
[redacted] Auditor
[redacted] Auditor
[redacted] Auditor

~~This Exhibit is UNCLASSIFIED//FOUO~~

This page intentionally left blank.

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

~~Further dissemination of this report outside the addressee organizations is PROHIBITED without the approval of the Inspector General.~~

INSPECTOR GENERAL REPORT

(U) Review of the President's Surveillance Program

ST-09-0002
29 June 2009

~~Derived From: STLW Classification Guide Dated: 12 January 2009 Declassify On: MR~~

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts inspections, audits, and investigations. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations; to provide intelligence oversight; to protect against fraud, waste, and mismanagement of resources; and to ensure that NSA/CSS activities are conducted in compliance with the Constitution, laws, executive orders, regulations, and directives. The OIG also serves as ombudsman, assisting all NSA/CSS employees and affiliates, civilian and military.

(U) INSPECTIONS

(U) The inspection function conducts management and program evaluations in the form of organizational and functional reviews, undertaken either as part of the OIG's annual plan or by management request. The inspection team's findings are designed to yield accurate and up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with laws and regulations; the recommendations for corrections or improvements are subject to followup. The inspection office also partners with the Inspectors General of the Service Cryptologic Elements to conduct joint inspections of the consolidated cryptologic facilities.

(U) AUDITS

(U) The internal audit function is designed to provide an independent assessment of programs and organizations. Performance audits evaluate the economy and efficiency of an entity or program, as well as whether program objectives are being met and operations are in compliance with regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) THE OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste and mismanagement. Investigations and Special Inquiries may be undertaken as a result or irregularities that surface during an inspection or audit; or at the initiative of the Inspector General.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

29 June 2009
IG-11051-09

TO: DISTRIBUTION

SUBJECT: (U) Review of President's Surveillance Program (ST-09-0002) — INFORMATION MEMORANDUM

1. (U//~~FOUO~~) This report summarizes our review of the President's Surveillance Program, as mandated by the Foreign Intelligence Surveillance Act Amendments Act of 2008.

2. (U//~~FOUO~~) For additional information, please contact my office on 301-688-6666. We appreciate the courtesy and cooperation extended to our staff throughout the review.

George Ellard

GEORGE ELLARD
Inspector General

DISTRIBUTION:

SID
OGC

(U) EXECUTIVE SUMMARY

(U) OVERVIEW

~~(TS//SI//NF)~~ For over a decade before the terrorist attacks on 11 September 2001, NSA used its SIGINT authorities to provide information in response to Intelligence Community requirements on terrorism targets. In late September 2001, when the Vice President asked the Director of Central Intelligence what more NSA could do with additional authority, NSA's Director identified impediments to enhancing SIGINT collection under existing authorities. He said that in most instances NSA could not collect communications on a wire in the United States without a court order. As a result, NSA's ability to quickly collect and report on a large volume of communications from foreign countries to the United States was impeded by the time-consuming court order approval process. Attempting to obtain court orders for [redacted] foreign telephone numbers and Internet addresses was impractical for collecting terrorist communications with speed and agility.

~~(TS//STLW//SI//OC/NF)~~ Counsel to the Vice President drafted the 4 October 2001 Authorization that established the President's Surveillance Program (PSP), under which NSA could routinely collect on a wire, for counterterrorism purposes, foreign communications originating or terminating in the United States. Under the PSP, NSA did not target communications with both ends in the United States, although some of these communications were incidentally collected.

~~(TS//STLW//SI//OC/NF)~~ The PSP gave NSA a capability to exploit a key vulnerability in terrorist communications. [redacted]

According to senior NSA leaders, the value of the program was that this SIGINT coverage provided confidence that someone was looking at the seam between foreign and domestic intelligence domains to detect and prevent attacks in the United States.

~~(TS//STLW//SI//OC/NF)~~ NSA's Director said that SIGINT reporting on an extremist linked [redacted] "probably saved more lives" than any other PSP information and is, therefore, the most important SIGINT success of the PSP. NSA analysis [redacted]

~~(TS//STLW//SI//OC/NF)~~ Knowledge of the Program was strictly limited at the express direction of the White House, and NSA's Director needed White House approval to inform members of Congress about Program activity. Between 25 October 2001 and 17 January 2007, General Michael V. Hayden and Lieutenant General Keith B. Alexander conducted [redacted] PSP briefings for members of Congress and staff.

~~(TS//STLW//SI//OC/NF)~~ NSA activity conducted under the PSP was authorized by Foreign Intelligence Surveillance Court (FISC) orders by 17 January 2007, when NSA stopped operating under PSP authority. The NSA Office of the Inspector General (OIG) detected no intentional misuse of Program authority.

(U) HIGHLIGHTS

- **(U) PSP establishment, implementation, and product**

~~(TS//STLW//SI//OC/NF)~~ NSA began PSP operations on 6 October 2001. Although the Director of NSA was "comfortable" exercising the new authority and believed that it was lawful, he realized that it would be controversial. Under the PSP, NSA issued over [redacted] reports. This included [redacted] reports based on collected metadata, which was defined in the Authorization as [redacted] It also included [redacted] reports [redacted]

~~(TS//STLW//SI//OC/NF~~) NSA's PSP products, all of which were sent to CIA and FBI, were intended for intelligence purposes to develop investigative leads and were not to be used for judicial purposes. [redacted]

[redacted] and NSA had no mechanism to track and assess the effectiveness of PSP reporting.

- **(U) Access to legal reviews and program information**

  ~~(C//NF)~~ NSA's General Counsel and Inspector General were not permitted to read the 2001 DoJ, Office of Legal Counsel opinion on the PSP, but they were given access to draft 2004 Office of Legal Counsel opinions. Knowledge of the PSP was strictly controlled by the White House. Between 4 October 2001 and 17 January 2007, [redacted] people were cleared for access to PSP information.

- [redacted]

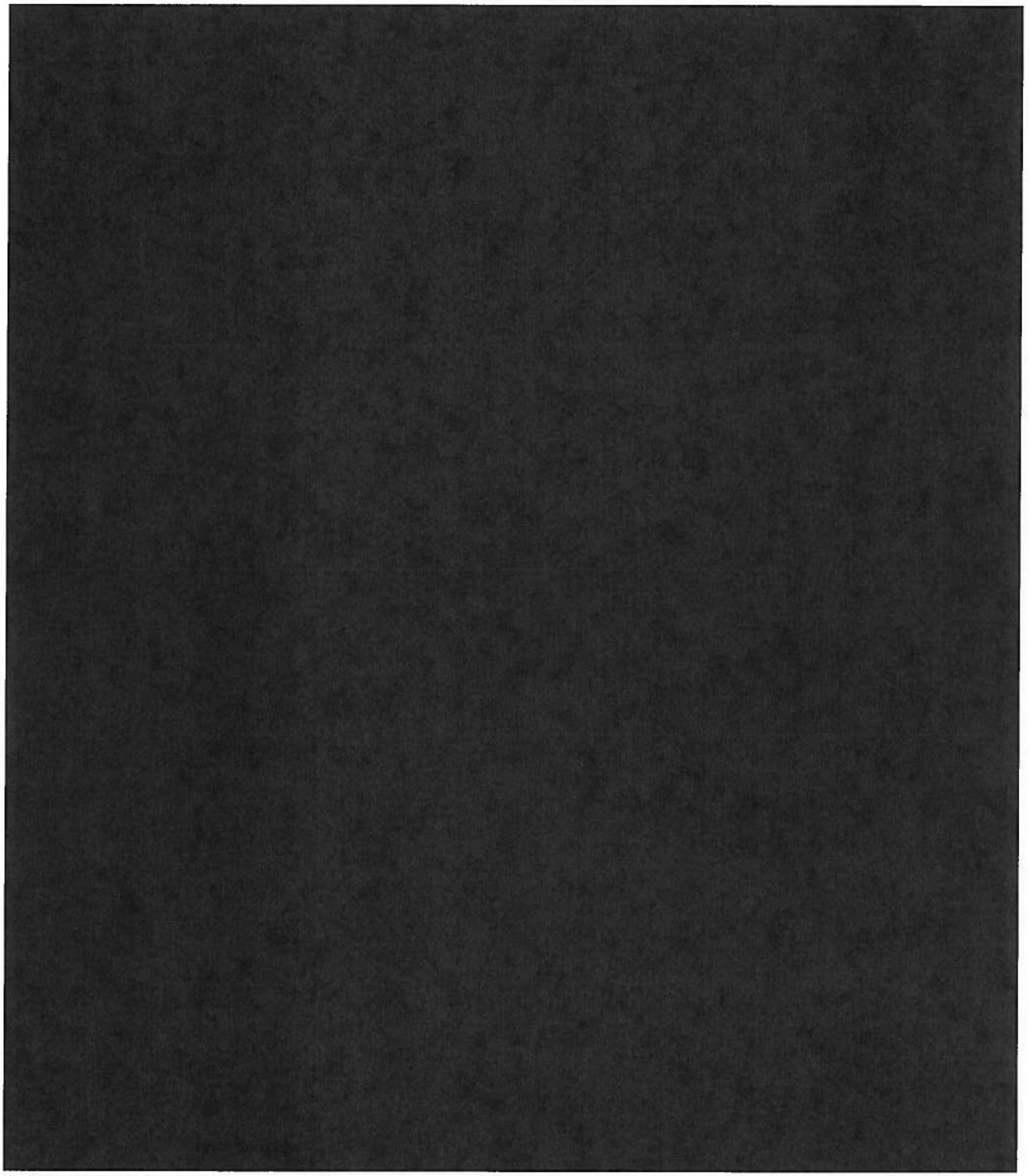
- **(U) NSA-FISC interaction and transition to court orders**

  ~~(TS//STLW//SI//OC/NF)~~ NSA's PSP-related interaction with the FISC was primarily briefings to presiding judges, beginning in January 2002. Interaction increased when NSA and the DoJ began to transition PSP activities to FISC orders. After parts of the program had been publicly revealed in December 2005, all members of the FISC were briefed. NSA's PSP authorized collection of bulk Internet metadata, telephony business records, and the content of communications transitioned to FISC orders on 14 July 2004, 24 May 2006, and 10 January 2007, respectively.

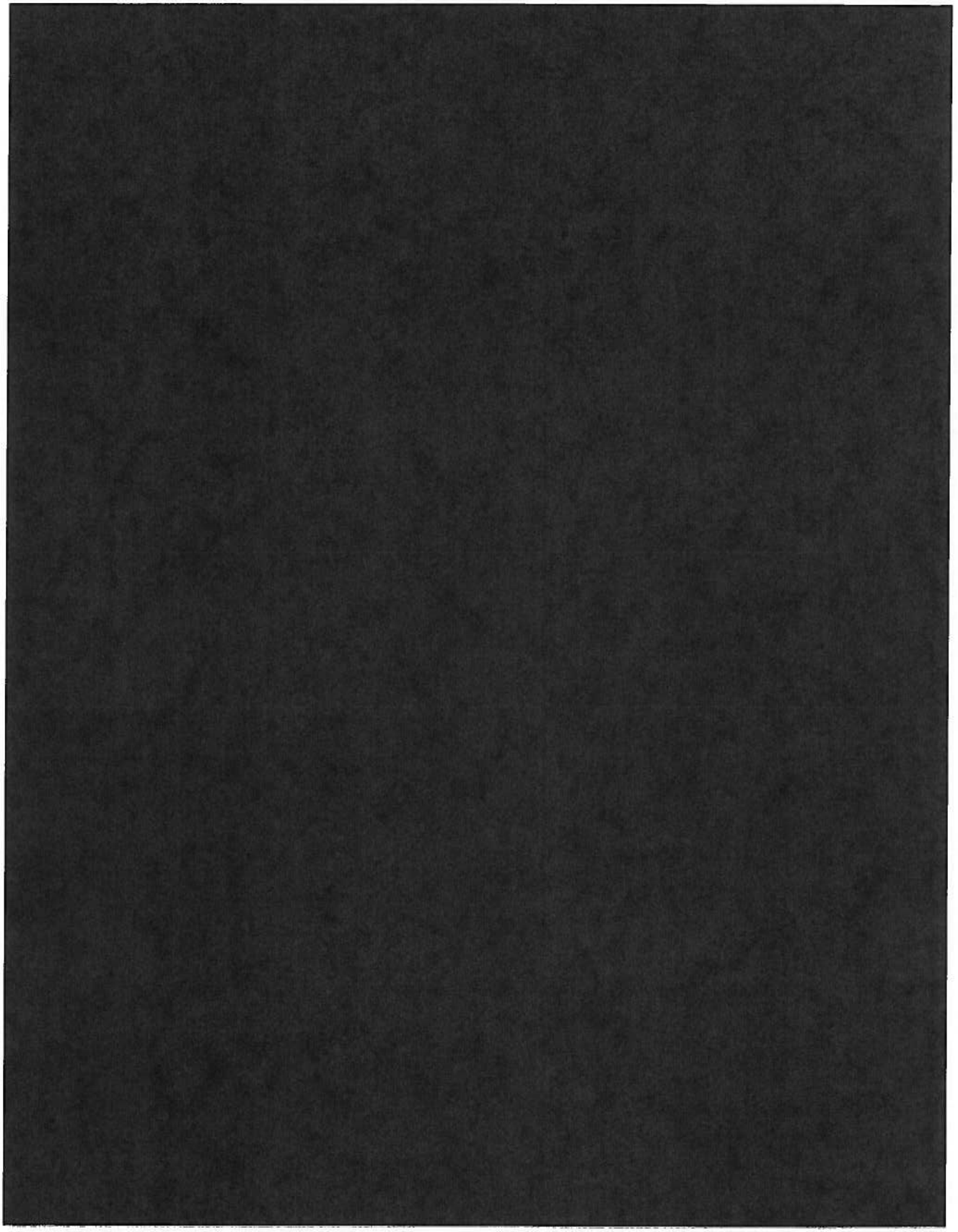
- **(U) Program oversight at NSA**

  ~~(C//NF)~~ NSA's Office of General Counsel and Signals Intelligence Directorate provided oversight of NSA PSP activities from October 2001 to January 2007. NSA OIG oversight began after the IG was cleared for PSP information in August 2002.

This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.

[redacted]

~~(S//NF)~~ For years before the 11 September 2001 terrorist attacks in the United States, NSA had been using its authorities to focus the United States Signals Intelligence (SIGINT) System on foreign intelligence targets, including terrorism, in response to Intelligence Community requirements. After the attacks, NSA adjusted SIGINT collection, in accordance with its authorities, to counter the terrorist threat within the United States. In late September, the Vice President asked the Director of Central Intelligence (DCI) if NSA could do more to prevent another attack. NSA's Director responded by describing impediments to SIGINT collection of terrorist-related communications to the Vice President. Counsel to the Vice President used the information about impediments to draft the Presidential Authorization that established the PSP.

(U) SIGINT Efforts against Terrorists before 11 September 2001

~~(C//NF)~~ For over a decade before terrorists attacked the United States in September 2001, NSA was applying SIGINT assets against terrorist targets in response to Intelligence Community requirements. The Signals Intelligence Directorate (SID) Counterterrorism (CT) Product Line led these efforts in accordance with SIGINT authorities, which defined what NSA could and could not do against SIGINT targets.

(U) Authorized SIGINT activity in September 2001

(U) NSA was authorized by Executive Order (E.O.) 12333, *United States Intelligence Activities*, 4 December 1981, as amended, to collect, process, and disseminate SIGINT information for foreign intelligence and counterintelligence purposes in accordance with DCI guidance and to support the conduct of military operations under the guidance of the Secretary of Defense. NSA and other Intelligence Community agencies were required by E.O. 12333 to conduct intelligence activities in accordance with U.S. law and other E.O. 12333 provisions.

(U) Both DoD regulation and NSA/Central Security Service (CSS) policy implemented NSA's authorities under E.O. 12333 and specified procedures governing activities that affect U. S. persons (DoD Regulation 5240.1-R, December

1982, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons* and NSA/CSS Policy 1-23, 11 March 2004, *Procedures Governing NSA/CSS Activities that Affect U. S. Persons).*

~~(S//SI//NF)~~ The policy of the U.S. SIGINT System is to collect, retain, and disseminate only foreign communications, which, in September 2001, were defined in NSA's legal compliance procedures (described below) as communications having at least one communicant outside the United States or entirely among foreign powers or between a foreign power and officers or employees of a foreign power. All other communications were considered domestic communications. NSA could not collect communications from a wire in the United States without a court order unless they originated and terminated outside the United States.

~~(S//SI//NF)~~ In 2001, NSA's authority to collect foreign communications included the Director of NSA's authority to approve targeting communications with one communicant in the United States, if technical devices (such as [redacted]) could be employed to limit acquisition of communications to those in which the target is a non-U.S. person located outside the United States, [redacted] or [redacted]

~~(S//SI//NF)~~ NSA's Director could exercise this authority, except when the collection was otherwise regulated, for example, under FISA for communications collected from a wire in the United States.

(U) NSA safeguards to protect U.S. persons' Constitutional rights

(U) The Fourth Amendment to the U.S. Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government.[1] United States Signals Intelligence Directive (USSID) SP0018, *Legal Compliance and Minimization*

[1] ~~(C//NF)~~ USSID SP0018 defines a U.S. person as a citizen of the United States, an alien lawfully admitted for permanent residence in the United States, unincorporated groups or associations a substantial number of the members of which constitute either of the first two groups, or corporations incorporated in the United States, including U.S. flag non-governmental aircraft or vessels, but not including those entities openly acknowledged by a foreign government to be directed and controlled by them.

Procedures, 27 July 1993, prescribes policies and minimization procedures and assigns responsibilities to ensure that United States SIGINT System missions and activities are conducted in a manner that safeguards U.S. persons' Constitutional rights. (See Appendix G.)

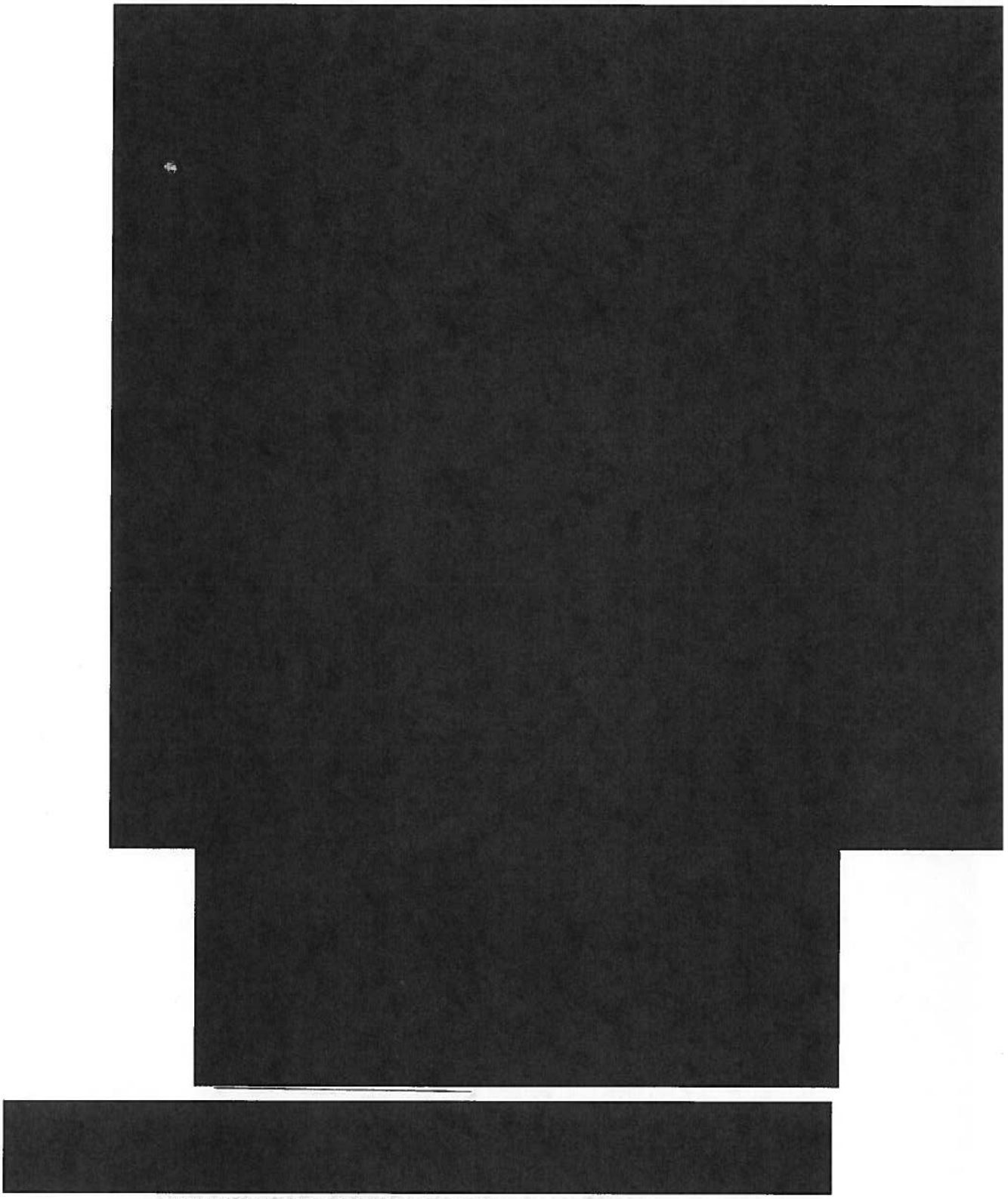
~~(S//SI//NF)~~ During the course of normal operations, NSA personnel sometimes inadvertently encounter information to, from, or about U.S. persons. When that happens, they must apply standard minimization procedures approved by the Attorney General in accordance with E.O. 12333 and defined in *USSID SP0018*. These procedures implement the constitutional principle of reasonableness by giving different categories of individuals and entities different levels of protection. They ensure that U.S. person information is minimized during collection, processing, dissemination, and retention of SIGINT by, for example, strictly controlling collection with a high risk of encountering U.S. person information and focusing all reporting solely on the activities of foreign entities and persons and their agents.

(U) NSA Director Used Existing Authorities to Enhance SIGINT Collection after Terrorist Attacks

[redacted]

[redacted]

APPROVED FOR PUBLIC RELEASE



[redacted]

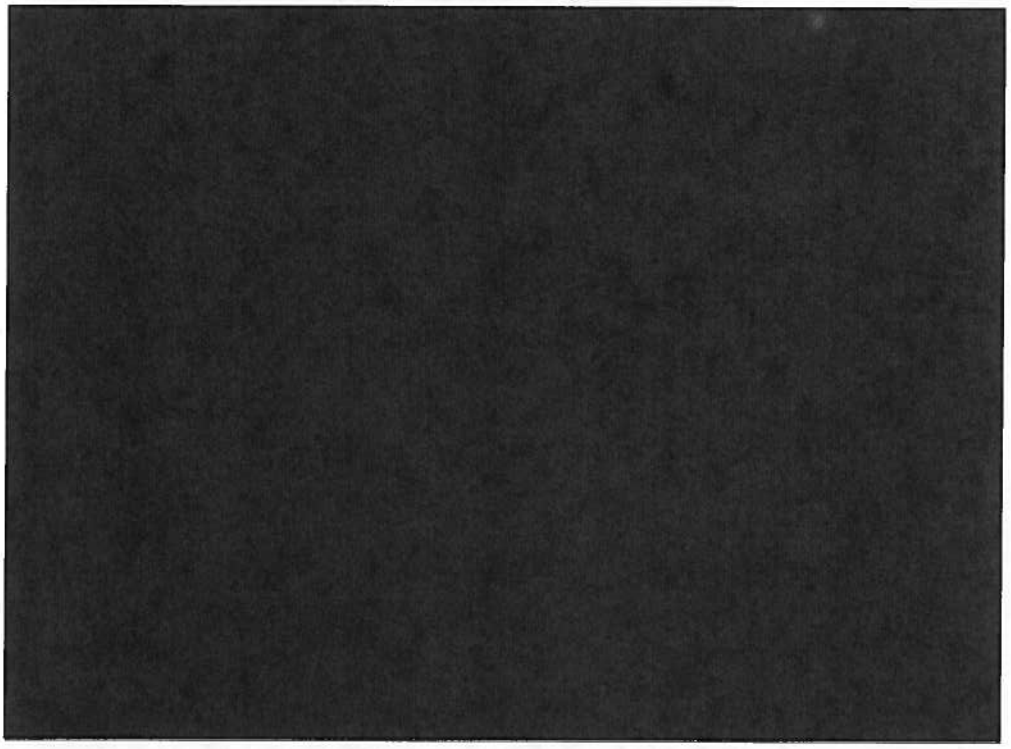
~~(S//NF)~~ In Oval Office Meeting, DCI Explained NSA Director's Decision to Expand Operations under Existing SIGINT Authorities

(U//~~FOUO~~) General Hayden recalled that in late September 2001, he told Mr. Tenet about NSA actions under E.O. 12333 to counter the terrorist threat. Mr. Tenet shared that information with the White House in an Oval Office meeting.

(U//~~FOUO~~) We did not interview Mr. Tenet or White House personnel during this review. We asked the White House to provide documentation of meetings at which General Hayden or NSA employees discussed the PSP or the Terrorist Surveillance Program with the President, Vice President, or White House personnel, but we did not receive a response before this report was published. Therefore, information about the sequence of events leading up to the establishment of the PSP comes from interviews of NSA personnel.

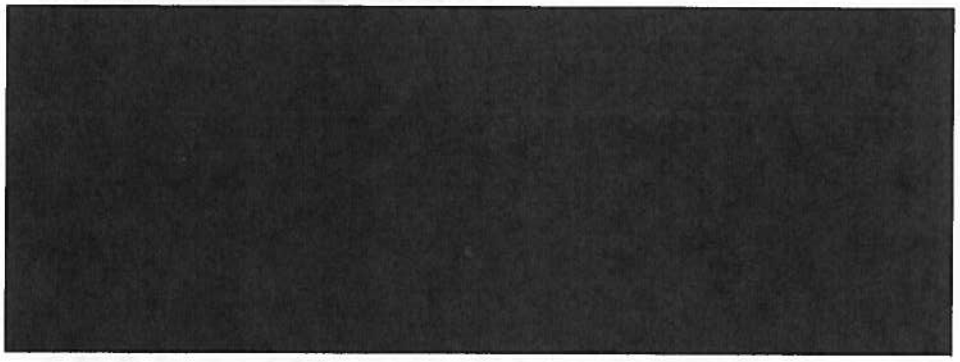
(U) Vice President Asked What Other Authorities NSA Needed

[redacted]



~~(S//NF)~~ NSA Options to Improve SIGINT Collection Could Not Fill Intelligence Gaps on Terrorist Targets

(U) FISA Amendments Considered



~~(S//NF)~~ General Hayden said that, in his professional judgment, NSA could not get the needed collection using the FISA. The process for obtaining court orders was slow, and it involved extensive coordination and separate legal and policy reviews by several agencies. Although an emergency authorization provision permitted 72 hours of surveillance without a court order, it did not allow the government to undertake surveillance immediately. Rather, the Attorney General had to ensure that emergency surveillance would

satisfy the standards articulated in the FISA and be acceptable to the FISC.

[redacted]

~~(S//SI//NF)~~ Under its authorities, NSA had no other options for the timely collection of communications of suspected terrorists when one end of those communications was in the United States and the communications could only be collected from a wire or cable in the United States.

(U//~~FOUO~~) NSA Director Described to the Vice President the Impediments to Improved SIGINT Collection against Terrorist Targets

[redacted]

[4] ~~(TS//SI//NF)~~ According to NSA OGC, DoJ has since agreed with NSA that simply processing communications metadata in this manner does not constitute electronic surveillance under the FISA.

(U//~~FOUO~~) After two additional meetings, the Vice President asked General Hayden to work with his Counsel, David Addington. Because early discussions about expanding NSA authority were not documented, we do not have records of attendees or specific topics discussed at General Hayden's meetings with White House representatives.

III. (U) THE PRESIDENTIAL AUTHORIZATIONS

[redacted]

~~(TS//STLW//SI//OC/NF)~~ Between 4 October 2001 and 8 December 2006, President George W. Bush signed 43 Authorizations, two modifications, and one document described as [redacted] The authorizations were based on the President's determination that after the 11 September 2001 terrorist attacks in the United States, an extraordinary emergency existed for national defense purposes. The Authorization documents contained the terms under which NSA executed special Presidential authority and were titled *Presidential Authorization for Specified Electronic Surveillance Activities during a Limited Period to Detect and Prevent Acts of Terrorism within the United States.* They were addressed to the Secretary of Defense.

(U) SIGINT Activity Permitted under the PSP

[redacted]

[redacted]

[redacted]

~~(TS//STLW//SI//OC/NF)~~ The authorizations changed over time, first eliminating the possibility that the Authority could be interpreted to permit collection of communications with both ends in the United States and adding an additional qualification that metadata could be collected for communications related to international terrorism or activities in preparation for international terrorism.[7] [redacted]

~~(TS//STLW//SI//OC/NF)~~ Starting in March 2004, the authorizations underwent several adjustments related to DoJ's Office of Legal Counsel's review of the Authority. [redacted] When these two clarifications were added to the 11 March 2004 and subsequent authorizations, an accompanying statement added that these clarifications had been previously understood and implemented by NSA and that they applied to past and future activities. Al-Qa'ida (also spelled al-Qaeda) was specified as a target for content collection [redacted] and NSA's authority to acquire [redacted] Finally, as a result of a subsequent change, NSA's authority to collect [redacted] but only for [redacted] with [redacted] thus [redacted]

~~(TS//STLW//SI//OC/NF)~~ The definition of "terrorist groups" within the authorities was also refined, and, for a limited

---

[6] ~~(TS//SI//NF)~~ Metadata, as defined by the Authorization, is [redacted]

[7] (U) See Appendix B for information about the types of collection permitted.

period in 2004, NSA analysts were permitted to query [redacted]

~~(TS//SI//OC/NF)~~ According to General Hayden, the Authorization, for the most part, did not change the communications that NSA could collect, but did change the location from which the Agency could collect them by permitting collection [redacted] in the United States. Without that authorization, [redacted]

[redacted]

(U) NSA Discussions about the Lawfulness of the Authorization

~~(TS//SI//NF)~~ NSA leaders believed that they could lawfully carry out the President's authorizations. However, they also recognized that the Program would be controversial and politically sensitive. This section describes how key NSA leaders—the Director, the NSA General Counsel, Deputy General Counsel, and Associate General Counsel for

Operations—concluded that the Program was legally defensible.

(U) Director of NSA

~~(TS//SI//NF)~~ Generals Hayden and Alexander stated that they believed the Authorization was lawful.

(U) General Hayden

~~(TS//SI//NF)~~ When asked how he had decided to execute an Authorization that some would consider legally and politically controversial, General Hayden said that NSA's highest ranking lawyers had advised him, collectively and individually, that the Program was lawful under the President's Article II powers. He said that three factors influenced his decision to implement the Authority. First, NSA would do exactly what the Authorization stated and "not one electron or photon more." Second, the Program was simply an expansion of existing NSA collection activities. Third, the periodic renewal of the Authorization would ensure that the threat continued to justify the Program.

~~(TS//SI//NF)~~ General Hayden said that as time passed, he determined that the Program was still needed. Specifically, he and NSA's Deputy Director reviewed the DCI threat memorandum for each reauthorization and judged that the threats continued to justify the Program.

~~(TS//SI//NF)~~ General Hayden said that no one at NSA expressed concerns to him or the NSA IG that the Authorization was not lawful. Most importantly, General Hayden said that no one outside NSA asserted that he should stop the Program. He occasionally heard concerns from members of Congress, but he sensed general support for the Program from those he briefed outside NSA. He emphasized that he did not just "flip through slides" during briefings. He wanted to ensure that attendees understood the Program; consequently, briefings lasted as long as the attendees wanted.

(U) General Alexander

~~(TS//STLW//SI//OC/NF)~~ When Lieutenant General Keith B. Alexander became NSA/CSS Director in mid-2005, some of the more controversial legal questions surrounding the Authorization had been settled. [redacted] the Office of Legal Counsel had

reviewed its initial opinion and determined that the remaining three types of collection were legally supportable.

(U) NSA Office of General Counsel

~~(TS//SI//NF)~~ After the Authorization was signed on 4 October 2001, NSA's highest ranking attorneys, the NSA General Counsel and Deputy General Counsel, as well as the Associate General Counsel for Operations, orally advised General Hayden that the Authorization was legal

(U) General Counsel

~~(TS//SI//NF)~~ After having received the Authorization on 4 October 2001, General Hayden asked NSA General Counsel Robert Deitz if it was lawful. Mr. Deitz said that General Hayden understood that the Attorney General had already certified its legality by signing the Authorization, but General Hayden wanted Mr. Deitz's view. Mr. Deitz said that on 5 October he told General Hayden that he believed the Authorization to be lawful. He added that he emphasized to General Hayden that if this issue were before the Supreme Court, it would likely rule, although not unanimously, that the Authorization was legal.

(U) Associate General Counsel for Operations

~~(TS//SI//NF)~~ On 5 October 2001, the General Counsel consulted the Associate General Counsel for Operations at his home by secure telephone. The Associate General Counsel for Operations was responsible for all legal matters related to NSA SIGINT activities. According to the General Counsel, he had not yet been authorized to tell the Associate General Counsel about the PSP, so he "talked around" it and did not divulge details. The Associate General Counsel was given enough information to assess the lawfulness of the concept described, but records show that he was not officially cleared for the PSP until 11 October 2001. On Tuesday, 9 October, he told Mr. Deitz that he believed the Authorization was lawful, and he began planning for its implementation.

(U) Deputy General Counsel

~~(TS//SI//NF)~~ The Deputy General Counsel was cleared for the PSP on 11 October 2001. He reviewed the Authorization with Mr. Deitz and the Associate General Counsel for Operations and also concluded that it was lawful.

(U) Discussions on Legality

~~(TS//SI//NF)~~ OGC attorneys said that their discussions about the Program's lawfulness took into account the severity of the 11 September attacks and the fear that foreign persons were in the United States planning attacks. The NSA attorneys concluded that the Authorization was lawful. Given the following factors, the General Counsel said the Authorization was constitutional and did not violate FISA.

[redacted]

- ~~(S//NF)~~ FISA was not a realistic means of addressing the terrorist threat inside the United States because the process lacked speed and agility.
- (U//~~FOUO~~) The Authorization was a temporary 30-day grant of authority.
- (U//~~FOUO~~) The statute allowed such an exception, or, to the extent that it did not, it was unconstitutional.

~~(TS//SI//NF)~~ The NSA attorneys determined that the President could issue the Authorization through his authority under Article II of the Constitution to perform warrantless electronic surveillance for foreign intelligence purposes outside and inside the United States. This conclusion, they said, was supported by the concurring opinion in *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), and appellate cases.[8]

~~(TS//SI//NF)~~ The Congressional *Authorization of Use of Military Force* and the canon of constitutional avoidance, which requires a court to attempt to interpret issues so as to avoid constitutional questions, cemented OGC's belief that the President's interpretation of Article II authority had legal merit.

---

[8](U) *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v Buck*, 548 F.2d 871 (9th Cir. 1977); *Zweibon v. Mitchell*, 516 F.2d 594 (DC Cir. 1975); *United States v. Brown* 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974), *cert. denied*, 419 U.S. 881 (1974).

~~(TS//SI//NF)~~ The Associate General Counsel for Operations described his position:

> ~~(TS//SI//NF)~~ Does Congress have the authority to limit Presidential Article II authority in foreign intelligence collection? Given the threat, this was a perfect storm of events—3,000 people killed, airplanes and buildings destroyed by foreign terrorists, an attack in the United States by a foreign terrorist organization. No one knew where the terrorists were or if there were more terrorists, and NSA had a collection capability unable to function because with the FISA, you cannot get [redacted] FISA orders needed to cover what you needed covered at that time to look for the terrorists. You go to the President and tell him that there is a statute that prevents you from doing something from a collection standpoint that may protect the United States from a future attack and that while the country is in danger, I have to adhere with a statute and can't get the amount of warrants I need. Any president is going to say there has got to be a way to do this – a federal law can't let me stand here and watch the country go down the tubes. Does the President have to abide by a statute depriving him of his authority and watch the country go down the tubes? Given the case law of five different circuits with the Supreme Court denying certiorari in two cases, there was good basis for deciding this.

~~(TS//SI//NF)~~ NSA OGC attorneys said that they did not prepare a formal written legal opinion because it was not necessary. The Attorney General had already certified the legality of the Program, and General Hayden had not asked for a written legal opinion. The attorneys also said that they did not have time to prepare a written legal opinion given the pace of operations.

~~(TS//SI//NF)~~ After having concluded that the Authorization was lawful, NSA attorneys believed it was important to ensure that NSA's implementation of the Program complied with the Authorization, that processes were well documented, and that strict controls and due diligence were embedded into the execution of the Program. Recognizing that the legal basis of the Program might become controversial, they said that they wanted to ensure that NSA's execution of the Authority would withstand scrutiny.

This page intentionally left blank.

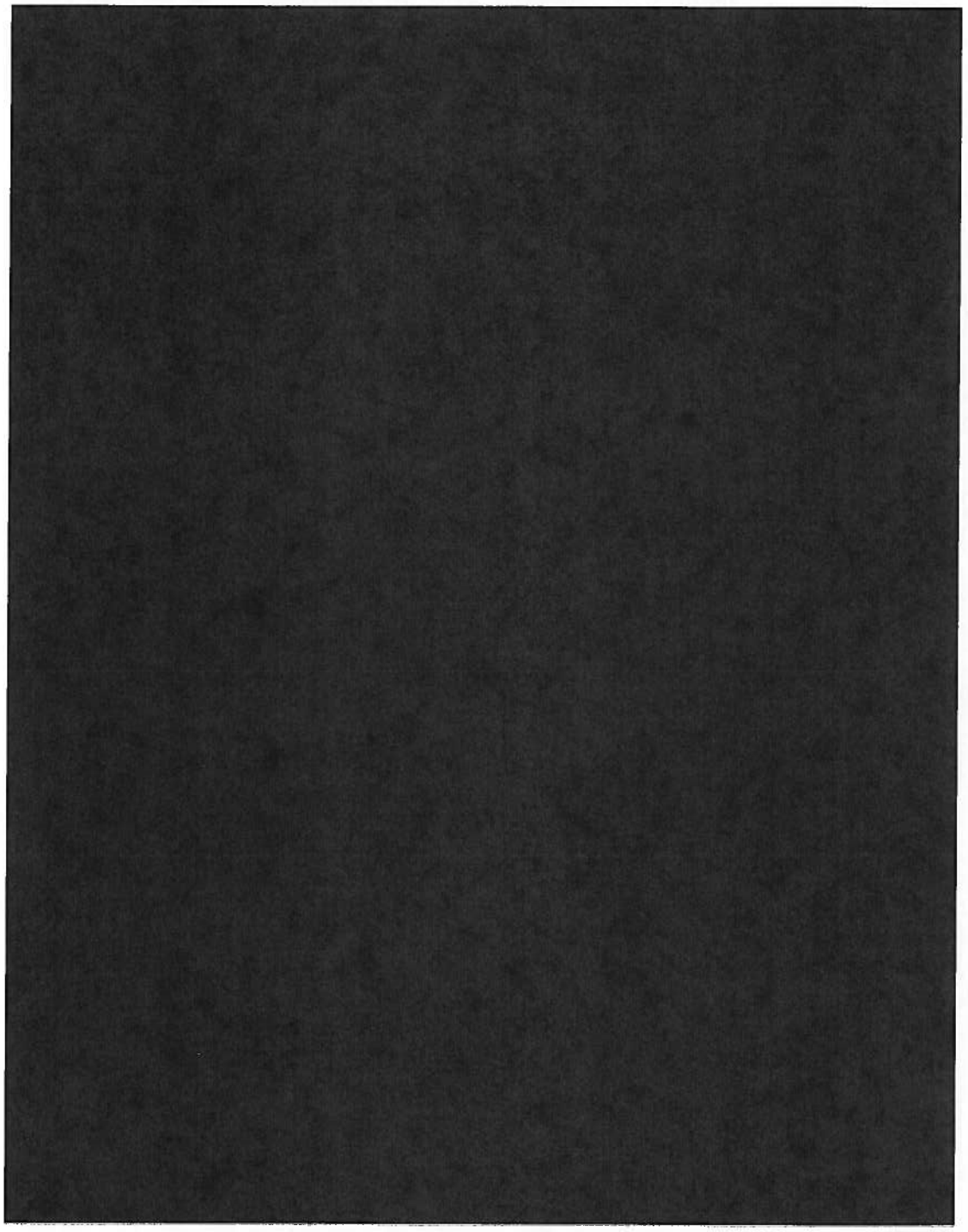
[redacted]

~~(TS//STLW//SI//OC/NF)~~ *NSA PSP operations began on 6 October 2001 and ended on 17 January 2007 and involved the collection, analysis, and reporting of two types of information: metadata and content. NSA assumed that the PSP was temporary and did not immediately formalize processes and procedures for operations, which were quickly set up to provide SIGINT on terrorist targets. As the Authorization continued to be renewed, NSA implemented special procedures to ensure that selectors used for metadata analysis and domestic selectors tasked for content collection were linked to al-Qa'ida, its associates, or international terrorism and that related decisions were documented. NSA did not target communications with both ends in the United States under PSP authority, although some of these communications were incidentally collected, and the OIG found no intentional violations of the Authorization. Over the life of the Program, NSA issued more than [redacted] products based on PSP data. According to senior NSA leaders, the value of the PSP was that SIGINT coverage provided confidence that someone was looking at the seam between the foreign and domestic intelligence domains to detect and prevent attacks in the United States.*

(U) NSA Begins PSP Operations

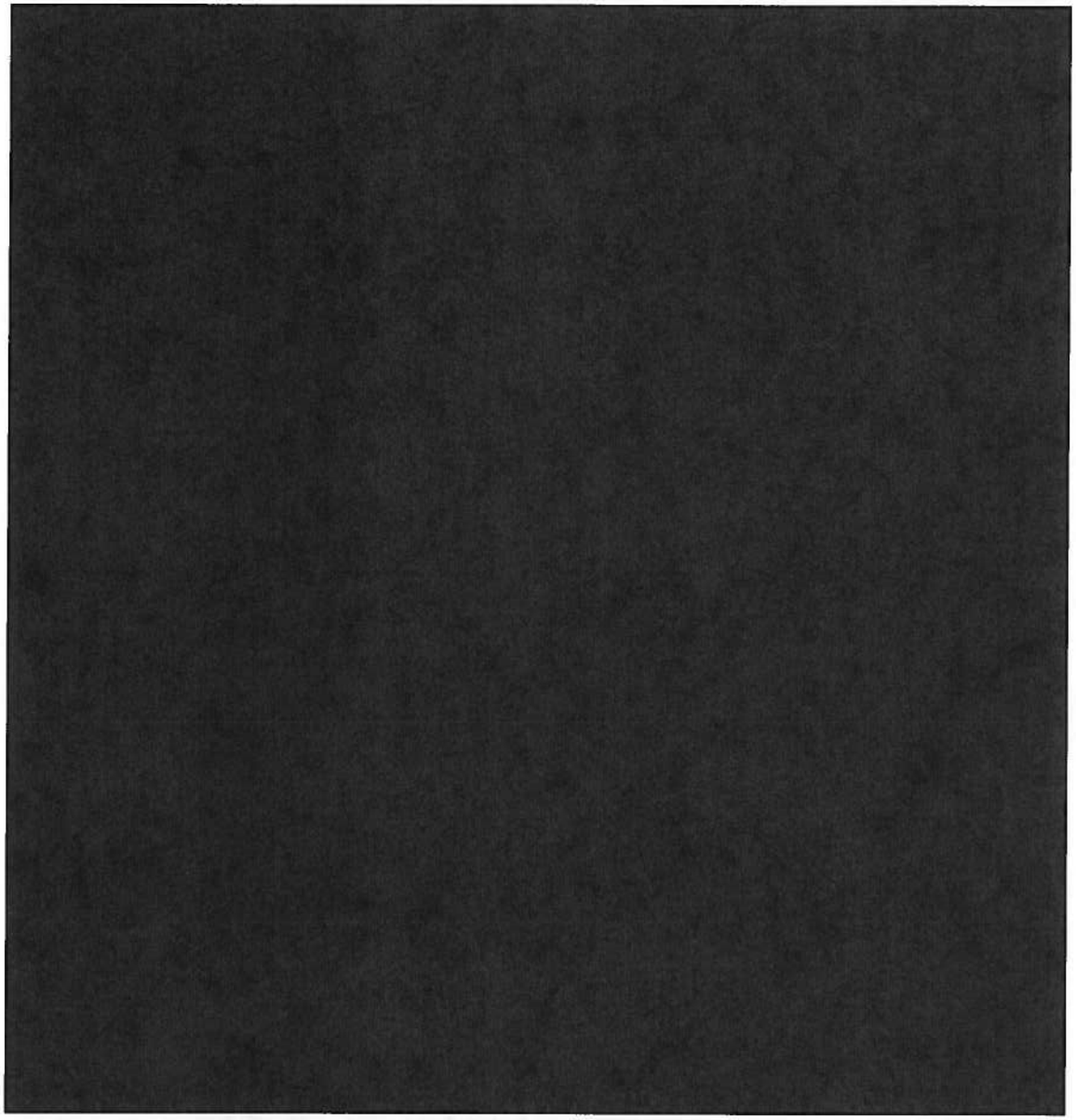
~~(S//NF)~~ On 4 October 2001, General Hayden received the initial Authorization and informed the SIGINT Director and other key personnel.

[redacted]



[9] ~~(S//NF)~~ A permanent cover term, STELLARWIND, was assigned to Program information on 31 October 2001

[10] ~~(S//NF)~~ [redacted]



~~(TS//SI//NF)~~ Authorization Renewed

~~(S//NF)~~ NSA leaders assumed the PSP would be temporary, so they did not establish processes and procedures for a long-term program, and they had plans to cease operations if the Authorization was not renewed. However, the President continued to renew the Authorization, and General Hayden stated that the DCI threat memoranda accompanying each renewal continued to justify the Program.

(U) FISA Authority Still not an Option in 2002

~~(TS//SI//NF)~~ In January 2002, senior NSA leaders still thought that neither the FISA court order process nor the infrastructure associated with FISA collection was suited to large numbers of targets [redacted]

[redacted]

[redacted]

~~(TS//SI//NF)~~ **NSA's First Attempt to Obtain FISA Authority on [redacted] Failed.**

~~(TS//SI//NF)~~ In September 2002, NSA attempted to obtain FISA authority to collect Internet and electronic wire communications of [redacted] using the standard process for seeking authority on foreign powers and foreign agents. Before preparing an application, NSA submitted a "Memorandum of Justification" to the [redacted][11]

[redacted]

~~(TS//SI//NF)~~ The request was prompted by a CT Product Line staff member, who explained that technical problems delayed NSA's receipt of e-mail collected through FISC orders that the FBI had obtained. [redacted] In one case, an FBI order listed only [redacted] terrorist agents of interest to NSA.

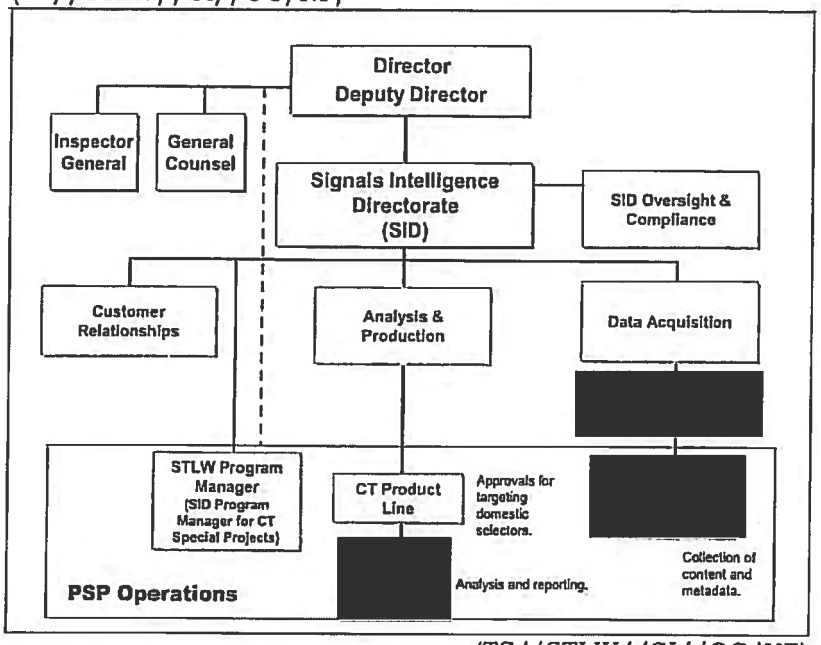
[redacted]

(U) NSA Structure for PSP Operations

[redacted]

(U//~~FOUO~~) NSA Organizational Structure for PSP Activity November 2004

~~(TS//STLW//SI//OC/NF)~~



~~(TS//STLW//SI//OC/NF)~~

(U) Chain of Command

~~(S//NF)~~ NSA's Director and Deputy Director exercised senior operational control and authority over the Program. According to NSA's Deputy Director, General Hayden handled "downtown" and the Deputy Director managed everything within NSA. The SIGINT Director at the start of the Program stated that once she was confident that the Program had appropriate checks and balances, she left direct management to the Director, Deputy Director, and the OGC. She noted that General Hayden took personal responsibility for the Program and managed it carefully. By 2004, specific roles related to collection, analysis, and reporting had been delegated to the SIGINT Director, who delegated management responsibilities to the Program Manager and mission execution responsibilities to the Chief of the CT Product Line and subordinate leaders.

[redacted]

[redacted]

(U) Coordination with FBI

~~(TS//STLW//SI//OC/NF)~~ On 24 January 2003, NSA, SID, and the FBI agreed to detail FBI personnel working under NSA SIGINT authorities to SID's [redacted] Under the agreement, detailees assisted with terrorism-related SIGINT metadata analysis, identified and disseminated terrorism-related SIGINT information meeting FBI foreign intelligence information needs, and facilitated NSA analyst access to FBI terrorism-related information.

[redacted]

[redacted]

~~(TS//SI//NF)~~ Minimization Procedures and Additional Controls on PSP Operations[12]

~~(TS//STLW//SI//OC/NF)~~ Management emphasized that the minimization rules required under non-PSP authorities also applied to PSP. The Authorization specifically directed NSA [redacted]

[12](U) Internal control, or management control, comprises the plans, methods, and procedures used to meet missions, goals, and objectives. It provides reasonable assurance that an entity is effective and efficient in its operations, reliable in its reporting, and compliant with applicable laws and regulations.

[redacted] NSA complied by applying USSID SP0018 minimization procedures. For example, and as described in the following sections:

- The collection of U.S. person information was minimized by [redacted]
- When analysts encountered U.S. person information, they handled it in accordance with minimization guidance, which included reporting violations or incidents.
- Dissemination of U.S. person information was minimized by requiring pre-release verification that the information was related to counterterrorism and necessary to understand the foreign intelligence or assess its importance.

~~(C//NF)~~ In addition, as PSP operations stabilized and the Authorization continued to be renewed, NSA management designed processes and procedures to implement the Program effectively while ensuring compliance with the Authorization and protecting U.S. person information. By April 2004, formal procedures were in place, many of which were more stringent than those used for non-PSP SIGINT operations. One analyst commented that the PSP "had more documentation than anything else [she] had ever been involved with." Examples of controls, some of which will be explained in more detail in the following sections of this report, include:

- ~~(TS//STLW//SI//OC/NF)~~ Approvals—Shift Coordinators approved foreign and domestic target selectors for metadata analysis. The Chief or Deputy of CT Product Line Chief or the Program Manager approved domestic selectors for content collection under the PSP.
- ~~(TS//STLW//SI//OC/NF)~~ Documentation—RFIs, leads, tasked domestic selectors, and tippers were tracked in the [redacted] Justifications for contact chaining were recorded, and justification packages and approvals for tasking domestic selectors for content collection were formally documented.

- ~~(TS//SI//NF)~~ Monitoring—Statistics on content tasking and reports were maintained and reviewed by SID, Oversight and Compliance by 2003. A CT Product Line employee stated: "... [N]owhere else did NSA have to report on selectors and how many selectors were rolled off [detasked] and why."

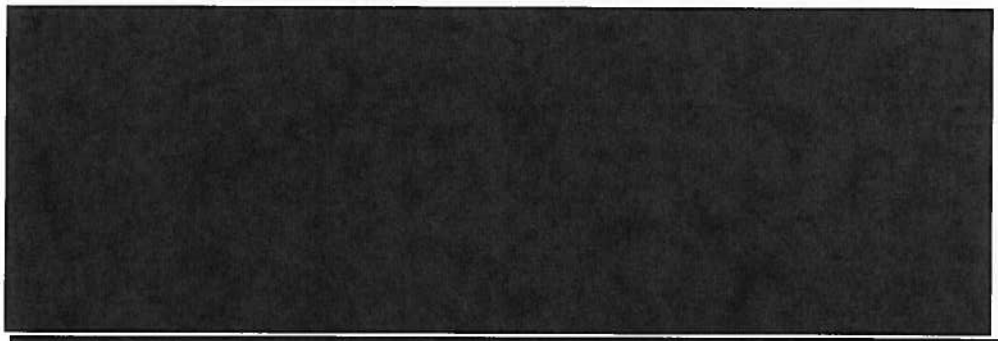
- (U//~~FOUO~~) OGC involvement—Personnel working under PSP authority noted that they had a continuous dialogue with the OGC on what was permissible under the Authorization. The Associate General Counsel for Operations confirmed that the OGC "was involved with the operations people day in and day out."

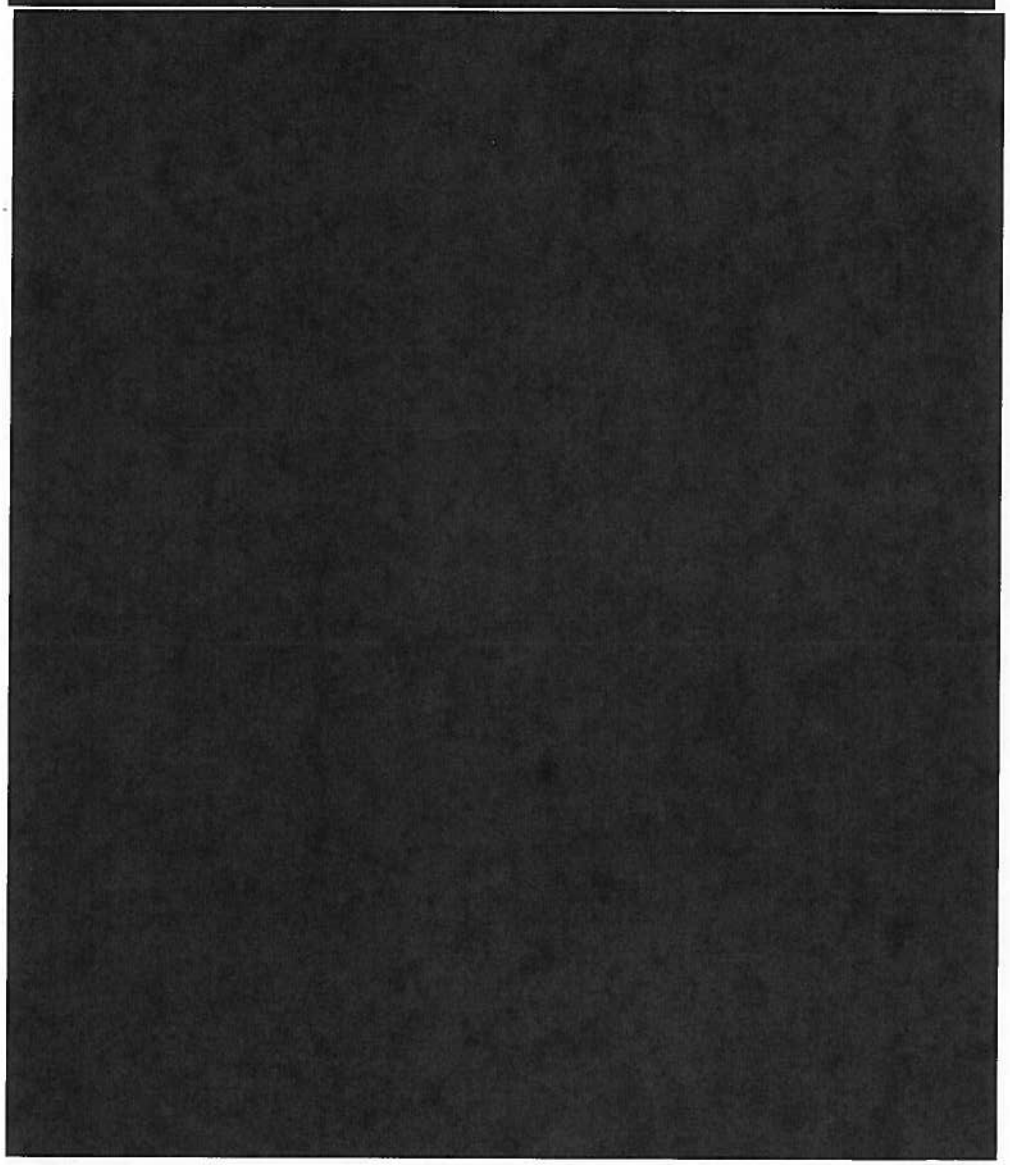
- (U//~~FOUO~~) Due Diligence Meetings—The PSP Program Manager chaired due-diligence meetings attended by operational, OIG, and OGC personnel. They discussed OIG and OGC reviews and Program challenges, processes, procedures, and documentation.

~~(TS//SI//NF)~~ PSP Operations: Metadata

(TS//STLW//SI//OC/NF) The Authorization defines "metadata" as [redacted] For example, e-mail message metadata includes the sender and recipient e-mail addresses. It does not include the subject line or the text of the e-mail, which are considered content. Telephony metadata includes such information as the calling and called telephone numbers, but not spoken words.

[redacted]





~~(TS//SI//NF)~~ Process to Conduct Metadata Analysis

[redacted]

~~(TS//SI//NF)~~ Standards for Conducting Metadata Analysis

~~(TS//SI//NF)~~ During an OIG review in 2006, the Associate General Counsel for Operations described OGC's standards for complying with the terms of the Authorization when conducting metadata analysis and contact chaining.

~~(TS//SI//NF)~~ To conduct contact chaining under the PSP, the Authorization required that NSA meet one of the following conditions: 1) at least one party to the communication had to be outside the United States, 2) no party to the communication could be known to be a U.S. citizen, or 3) based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there were specific and articulable facts giving reason to believe that the communication relates to international terrorism or activities in preparation therefor. The Associate General Counsel for Operations said that OGC's guidance was more stringent than the Authorization in that the OGC always required that the third condition be met before contact chaining began. Analysts were required to establish a link with designated groups related to international terrorism, al-Qa'ida, or al-Qa'ida affiliates.[14]

~~(S//NF)~~ The Associate General Counsel for Operations said that establishing a link to international terrorist groups or al-Qa'ida and its affiliates met the Authorization's requirement that all activities conducted under the PSP be for the purpose of detecting and preventing terrorist acts within the United States. He explained that because the President had determined that [redacted] international terrorist groups [redacted] al-Qa'ida presented a threat within the United States, regardless of where members were located, linking a target selector to such groups established that the collection was for

---

[13](U) Smith v. Maryland, 442 U.S. 735, 742 (1979).
[14](TS//SI//NF) [redacted]

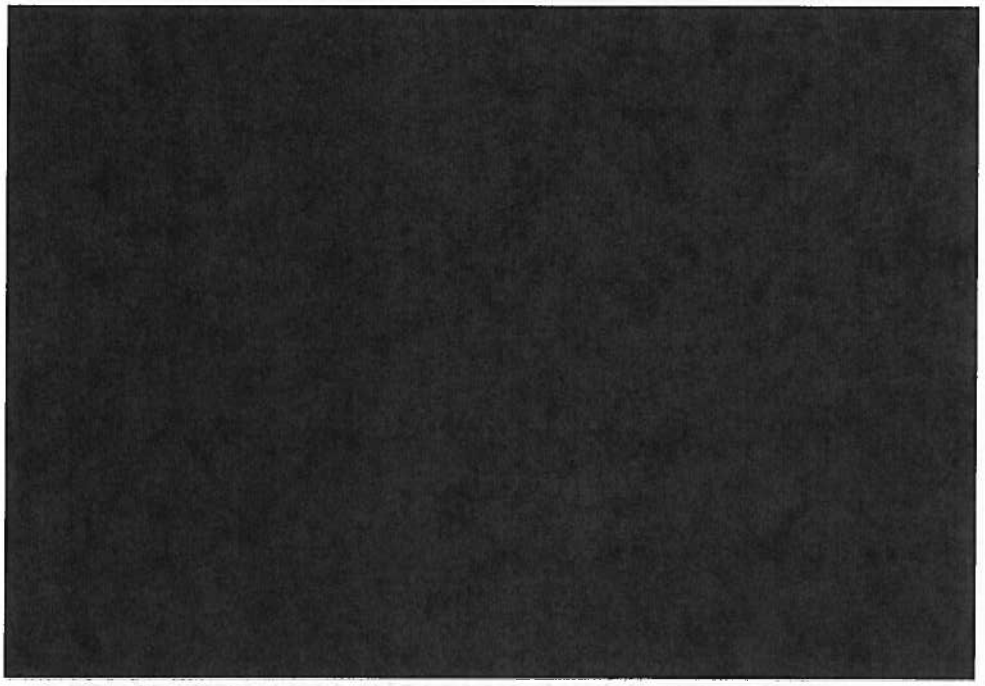
the purpose of detection and prevention of terrorist acts within the United States.

~~(TS//SI//NF)~~ In a 2005 Program memorandum, NSA OGC defined the NSA standard for establishing a link to al-Qa'ida under the PSP. NSA could target selectors when "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are reasonable grounds to believe a party to such communication is an agent of al-Qa'ida, or a group affiliated with al-Qa'ida."

> ~~(TS//STLW//SI//OC/NF)~~ Facts giving rise to "reasonable grounds for belief" means reliable facts in NSA's possession, either derived from its signals intelligence activity, or facts provided to NSA by another government department or agency, or facts reliably in the public record (e.g., a newspaper article). Whatever the source of information, the key is that NSA is basing its determination on articulable facts, not on bare assertions made by someone else. We need evidence, rather than conclusions. Thus a mere statement that person X is a member of al Qaeda, without more information, will not suffice as a justification for chaining or for content tasking. Instead we need to know what facts have led NSA, or another agency, or the press, etc., to that conclusion. Focus on the facts and determine whether they lead to a conclusion, rather than accepting someone else's conclusion. If you don't have enough facts to make a determination, ask for them.
>
> ~~(TS//STLW//SI//OC/NF)~~ In addition, the standard does not require certain knowledge, or even necessarily a better than 50/50 chance that the user of a phone or e-mail is a member of al Qaeda or an affiliated organization. It requires only that a reasonable and prudent person exercising good judgment would conclude that there are grounds for believing the thing to be proved. It is not mere hunch or mere suspicion, nor is it proof beyond a reasonable doubt or even a preponderance of the evidence; rather, the standard requires some degree of concrete and articulable evidence or information on which to base a conclusion.

(U) Approvals for Metadata Analysis

[redacted]



~~(TS//SI//NF)~~ If the standard for establishing a link to al-Qa'ida could not be met based solely on the information provided in the RFI or lead, analysts could search NSA and Intelligence Community databases and chain under non-PSP authorities to find additional facts to substantiate the link.

~~(TS//SI//NF)~~ Shift coordinators were not required to approve all alert-list selectors that might have generated [redacted] chaining. One individual, the equivalent of a shift coordinator, managed and monitored the alert process.

~~(TS//SI//NF)~~ When NSA personnel identified erroneous metadata collection, usually caused by technical collection system problems or inappropriate application of the Authorization, minimization procedures required them to report the violation or incident through appropriate channels and to delete the collection from all NSA databases. Early in the Program, NSA reported three violations in which the Authorization was not properly applied and took measures to correct them.

- ~~(TS//STLW//SI//OC/NF)~~ In [redacted] NSA [redacted] chained on numbers associated with [redacted] In this case, the target was foreign, but there was no link to terrorism.

- ~~(TS//STLW//SI//OC/NF)~~ In [redacted] NSA chained on a domestic telephone number provided by the FBI that was related to a [redacted] investigation. In this case, the target posed a terrorist threat inside the United States, but there was no known link to international terrorism.

- ~~(TS//STLW//SI//OC/NF)~~ In [redacted] NSA chained on metadata based on two telephone numbers provided by FBI related [redacted] While the selectors were associated with international terrorism, [redacted] did not pose a threat of terrorist attacks inside the United States.

~~(TS//SI//NF)~~ Bulk Metadata Needed for Effective Contact Chaining

~~(TS//STLW//SI//OC/NF)~~ Effective contact chaining requires large amounts of metadata, sometimes called bulk metadata, because more data yields more complete chains. [redacted]

~~(TS//STLW//SI//OC/NF)~~ Under PSP authority, NSA obtained a daily average of approximately [redacted] telephony metadata records and an estimated [redacted] Internet metadata records. Metadata obtained under PSP authorities was stored in a protected database, to which only cleared and trained personnel were given access. NSA analysts were able to access and chain through metadata records, but they could view only records associated with an approved foreign intelligence target. This was a small fraction of the metadata available. For example, in August 2006, NSA estimated that only 0.000025 percent or one in every four million archived bulk telephony records was expected to be viewed by trained SIGINT analysts.[15]

---

[15] ~~(TS//SI//NF)~~ This estimate was presented in the August 2006 application for the Business Records Order, the FISC Order that permitted NSA's collection of call detail records. Although this estimate applies to collection and analysis of telephony metadata conducted under the Business Records Order, the same processes and

~~(TS//SI//NF)~~ PSP Operations: Content

~~(TS//STLW//SI//OC/NF)~~ [redacted] PSP content operations involved three separate activities: tasking selectors for content collection, collecting the content of communications associated with tasked selectors, and analyzing the content collected. To comply with the Authorization, NSA management combined standard minimization procedures and specially designed procedures to task domestic selectors, collect the resulting communications, and analyze and report the foreign intelligence they contained. Over the life of the Program, NSA tasked approximately [redacted] foreign and domestic selectors for content collection.

~~(TS//SI//NF)~~ Tasking Selectors for Content Collection

~~(TS//STLW//SI//OC/NF)~~ "Tasking" is the direct levying of SIGINT collection requirements on designated collectors. Analysts must task selectors to obtain a target's communications.

~~(TS//STLW//SI//OC/NF)~~ Under the PSP [redacted] Before NSA personnel tasked target selectors for PSP content collection, the Authorization required that target selectors comply with two criteria. First, they had to determine that [redacted] as described in guidance issued by OGC in 2005. Second, the purpose of the collection had to be the prevention and detection of terrorist attacks in the United States. The OGC provided the same guidance for tasking selectors for content collection as it had for contact chaining. Specifically, because the President had determined that al-Qa'ida presented a threat within the United States, regardless of where its members were located, linking a target selector to designated international terrorist groups or al-Qa'ida and its affiliates, established that the collection was for the purpose of detection and prevention of terrorist acts within the United States.

techniques were used under the PSP, making this a reasonable comparison. This estimate was based on data available in August 2006 and cannot be replicated.

~~(TS//SI//NF)~~ Approvals to Task Domestic Selectors for Content Collection

~~(TS//SI//NF)~~ NSA analysts determined whether foreign selectors met the Authorization criteria and tasked them without further approval. However, because NSA leadership considered selectors located in the United States to be extremely sensitive, the associated tasking process required extra documentation, reviews, and approvals than foreign selector tasking under the PSP.

[redacted]

[redacted]

[16](U) From 2005 to 2007, SID, Analysis and Production leadership titles changed. The Primary Production Center Manager became the primary approval authority for tasking packages.

[redacted]

~~(TS//SI//NF)~~ **Most Selectors Tasked for Content Collection Were Foreign.**

[redacted]

~~(TS//STLW//SI//OC/NF)~~ In 2008, NSA reported to a member of Congress that [redacted] domestic telephone numbers and [redacted] domestic Internet addresses were tasked for PSP content collection from October 2001 to January 2007. Domestic selectors were located in the United States and associated with al-Qa'ida or international terrorism and were not necessarily used by U.S. citizens. In a 2008 Attorney General Certification, NSA reported that [redacted] foreign telephone numbers and in excess of [redacted] foreign Internet addresses had been targeted from October 2001 through December 2006, which spans all but one month of the Program. NSA could not precisely estimate the number of

foreign Internet addresses targeted because the tools used by analysts before September 2005 did not accurately account for the number of individual addresses targeted.

~~(TS//SI//NF)~~ In 2006, the OIG Found that Justifications for Tasking Domestic Selectors Met Authorization Criteria.

~~(TS//STLW//SI//OC/NF)~~ During a 2006 review, the OIG found that all items in a randomly selected sample of tasked domestic selectors met Authorization criteria. Based on a statistically valid sampling methodology, the OIG was able to conclude with 95 percent confidence that 95 percent or more of domestic selectors tasked for PSP content collection could be linked to al-Qa'ida, its associates, or international terrorist threats inside the United States. Justification packages for all sample items tested were supported by one or more of the following types of information:

[redacted]

- Information associated with or obtained through FBI investigations.

(U) Process to Task Selectors

[redacted]

[redacted]

~~(TS//SI//NF)~~ In 2005, the OIG found that the largely manual process to task and detask selectors for content collection was unreliable. Specifically, the OIG found [redacted] errors when comparing records of domestic telephone numbers and Internet identifiers approved for PSP content collection as of November 2004 with those actually on collection. The errors consisted of selectors that had not been removed from collection after being detasked, had not been put on collection after having been approved, had been put on collection because of a typographical error, or had not been accurately recorded in the [redacted] In response to the OIG finding, management took immediate steps to correct the errors and set up a process to reconcile approved tasked selectors with selectors actually on collection.

~~(TS//SI//NF)~~ Collecting the Content of Communications

(U//~~FOUO~~) Collection refers to the process of obtaining communications after selectors associated with intelligence targets are tasked for collection at designated sites. Data collected under the PSP was stored in protected partitions in NSA databases. Access to the partitions was restricted to PSP-cleared personnel.

~~(TS//SI//NF)~~ The Authorization required that a collected communication originate or terminate outside the United States. NSA did not intentionally collect domestic communications under the PSP. [redacted] and the CT Product Line to ensure that collected data was as intended and authorized. According to PSP program officials, NSA's [redacted] Its purpose was to collect international communications. However, management stated that:

> There are no readily available technical solutions within the [redacted] to guarantee that no [domestic] calls will be collected. Issues of this kind inevitably arise from time to time in other SIGINT operations, as foreseen by Executive Order 12333, and are thus not peculiar to [the PSP].

~~(S//NF)~~ The Program Management Office identified four ways that NSA might have unintentionally collected non-target data:

- A target could have been correctly tasked using valid selectors, but, in addition to collecting the desired target communications, non-target communications were inadvertently collected.
- A valid target selector could have generated target-specific collection that ultimately proved the target not to be related to al-Qa'ida.
- A technical, human, or procedural error in the target identification or tasking process could have resulted in unintentional collection of communications not related to al-Qa'ida.
- Technical collection system problems could have resulted in unintentional collection of non-al-Qa'ida related targets, even when all steps in the target identification and tasking process had been properly executed.

~~(S//NF)~~ Over the life of the Program, NSA reported [redacted]ncidents of unintentional collection of domestic communications and [redacted]incidents in which the wrong selector had been tasked. (See Appendix F for details.) In those cases, personnel followed USSID SP0018 procedures and were given detailed instructions to report the violations or incidents, adjust tasking, and delete collection records from NSA and other databases.

~~(TS//SI//NF)~~ Analyzing the Content of Collected Communications

~~(TS//SI//NF)~~ Analysis of content collected under the PSP involved the same practices and techniques used in non-PSP operations. One NSA manager described the PSP as "just one more tool in the analysts' tool kit." [redacted] Collected communications were then transcribed, if necessary, and processed to make them useful for intelligence analysis and reporting. Analysis included not only listening to or reading the contents of a communication, but drawing on target knowledge, coordinating and collaborating with other analysts, and integrating collateral information, metadata, and information from databases and published intelligence

reports to determine whether the communications included foreign intelligence that was timely, unique, actionable, and reportable.

[redacted]

[redacted]

[redacted]

---

[17](U//~~FOUO~~) A serialized report is a formatted intelligence product produced pursuant to USSID CR1400 that has a reference serial number, contains foreign intelligence information derived from SIGINT, and goes to approved users of intelligence.

[18](~~TS//STLW//SI//OCNF~~) NSA issued [redacted] additional reports between 17 January 2007 and December 2008 that were based on analysis of data previously collected under PSP authority.

[redacted]

~~(TS//SI//NF)~~ **Metadata Analysis Reports (Tippers)**

~~(TS//STLW//SI//OC/NF)~~ Reports based on metadata analysis were referred to as "tippers." [redacted]

[redacted]

~~(TS//STLW//SI//OC/NF)~~ NSA retained documentation of the analysis, supporting customer request or lead information, and a description of the link to terrorism for tippers based on PSP collection. Documentation of analysis was not retained unless a tipper was written. Counterterrorism personnel updated information in a computer tracking system to reflect the disposition of all metadata analysis requests. From October 2001 through January 2007, NSA issued [redacted] tippers to FBI and CIA:

- [redacted] tippers were based on Internet metadata analysis.
- [redacted] tippers were based on telephony metadata analysis when telephone numbers had only direct contact (one degree of separation) with a known terrorist as defined by the Authorization.

- [redacted] tippers were based on more detailed telephony metadata analysis that included contacts with two degrees of separation from known terrorists.
- [redacted] tippers were based on telephony and Internet metadata analysis.

~~(TS//SI//NF)~~ Content Reports

~~(TS//STLW//SI//OC/NF)~~ PSP content reports contained NSA's analysis of communications [redacted]

(U//~~FOUO~~) Protection of U.S. Person Information in Reporting

~~(TS//SI//NF)~~ Before sending PSP reports to customers, NSA removed unnecessary U.S. person information, as required by minimization procedures in *USSID SP0018*. The CT Product Line reviewed PSP reports to ensure that they had been written in accordance with these procedures. SID's Oversight and Compliance office then reviewed PSP reports containing U.S. person information. Oversight and Compliance personnel reviewed U.S. person information in reports, determined if it was necessary to understand the foreign intelligence in the reports, and submitted recommendations for the inclusion of U.S. person information to SID, Chief of Information Sharing Services for final approval. For example, if an individual's name was not necessary to understand the foreign intelligence in the report, the name was deleted or changed to "a U.S. person."

~~(TS//SI//NF)~~ Oversight and Compliance did not review tippers based on metadata analysis. When NSA began to issue tippers based on the content of communications, SID adapted its procedures for the dissemination of U.S. person information. Additional Oversight and Compliance personnel were cleared for the Program to assist with reviews. They gave PSP and other terrorism reporting priority for review over other Agency reporting.

(U) Use of SIGINT Product

~~(TS//SI//NF)~~ As NSA's primary customers for PSP information, [redacted] All products included this statement:

> This information is provided only for intelligence purposes in an effort to develop potential investigative leads. It cannot be used in court proceedings, subpoenas, or for other legal or judicial purposes.

(U//~~FOUO~~) Value of the PSP

~~(TS//SI//NF)~~ Referring to portions of the PSP in 2005, General Hayden said there were probably no communications more important to NSA efforts to defend the nation than those involving al-Qa'ida. NSA collected communications when one end was inside the United States and one end was associated with al-Qa'ida or international terrorism in order to detect and prevent attacks inside the United States. General Hayden stated that "the program in this regard has been successful." During the May 2006 Senate hearing on his nomination to be CIA Director, General Hayden said that, had the PSP been in place before the September 2001 attacks, hijackers Khalid Almihdhar and Nawaf Alhazmi almost certainly would have been identified and located.

~~(TS//SI//NF)~~ In May 2009, General Hayden told us that the value of the Program was in knowing that NSA SIGINT activities under the PSP covered an important "quadrant" (terrorist communications between foreign countries and the United States). This coverage provided confidence that there were "not additional terrorist cells in the United States." NSA's Deputy Director, who was the SID Deputy Director for Analysis and Production on 11 September 2001, echoed

General Hayden's comment: "The value of the PSP was in the confidence it provided that someone was looking at the seam between the foreign and domestic intelligence domains."

~~(TS//SI//NF)~~ The former SID Deputy Director for Data Acquisition said that the possibility of a large terrorist presence in the United States [redacted] The PSP gave NSA a capability to exploit a key vulnerability in terrorists' communications: [redacted] With PSP authority, NSA could collect communications between [redacted] al-Qa'ida [redacted]

~~(TS//STLW//SI//OC/NF)~~ Current NSA Director General Alexander cited SIGINT reporting on [redacted] as the most important SIGINT success of the PSP. NSA analysis of PSP metadata and content collection placed [redacted], General Alexander said, "probably saved more lives" than any other PSP information produced by NSA because the information [redacted]

~~(TS//SI//NF)~~ From an operational standpoint, the PSP enabled NSA to:

- Support customers
- Provide SIGINT that contributed to customers' investigative work

[redacted]

~~(U//FOUO)~~ Support to Customers

~~(TS//SI//NF)~~ From April 2002 to January 2007, NSA responded to [redacted] and more than [redacted] from FBI. These numbers do not account for requests submitted before NSA began to use an automated tracking system in April 2002.

~~(TS//SI//NF)~~ Based on information obtained under PSP authority, NSA sent [redacted]

and FBI. In the early days of the Program, the FBI said that the large number of tippers from NSA was causing them unnecessary work because agents treated each tipper as a lead requiring action. General Hayden said that NSA's intention was that SIGINT information be added to FBI's knowledge base, not that the FBI act on each piece of information. When NSA realized that it was sending too much data to the FBI, the Agency made appropriate adjustments.

(U//~~FOUO~~) PSP Reporting Contributed to Customers' Investigative Work.

~~(TS//STLW//SI//OC/NF)~~ [redacted] For example, an FBI briefing dated 4 May 2006 stated that "STELLARWIND continues to provide timely and carefully vetted intelligence to support FBI's investigations in connection with [redacted] operations]."

~~(TS//STLW//SI//OC/NF)~~ [redacted] FBI did not routinely provide feedback on NSA reporting under the PSP, and NSA had no mechanism to track and assess the effectiveness of SIGINT reporting in general or PSP reporting in particular.[19] Tracking PSP contributions was also difficult because customers did not know that [redacted] General Hayden noted that success stories decreased over time as intelligence became more integrated and it became more difficult to attribute success to any one activity.

~~(TS//STLW//SI//OC/NF)~~ The Program Management Office provided the following examples of PSP reporting that helped redirect FBI resources [redacted] viewed as vulnerable to terrorism targeting. The examples also include cases in which NSA provided reporting that contributed to FBI investigations, FBI confidential human sources, FISA warrants, arrests, and convictions.

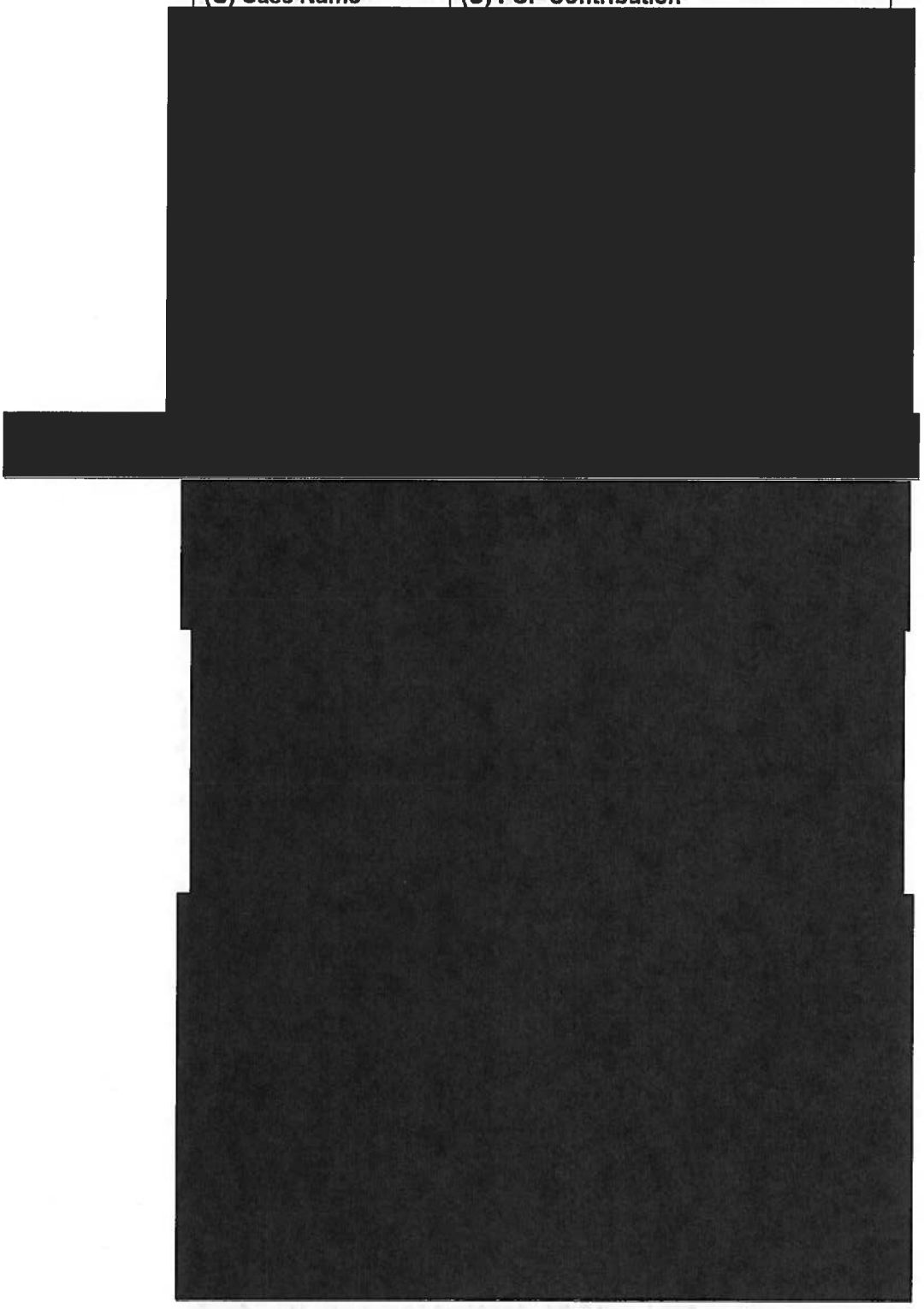
---

[19] ~~(C//NF)~~ In July 2007, SID initiated a formal effort to assess the effectiveness of its CT efforts. By the fall of 2007, that effort was struggling.

(U) Case Name	(U) PSP Contribution
[redacted]	

(U) Case Name	(U) PSP Contribution
[redacted]	

(U) Case Name	(U) PSP Contribution



(U) PSP Information	(U) Description of SIGINT Reporting
[redacted]	

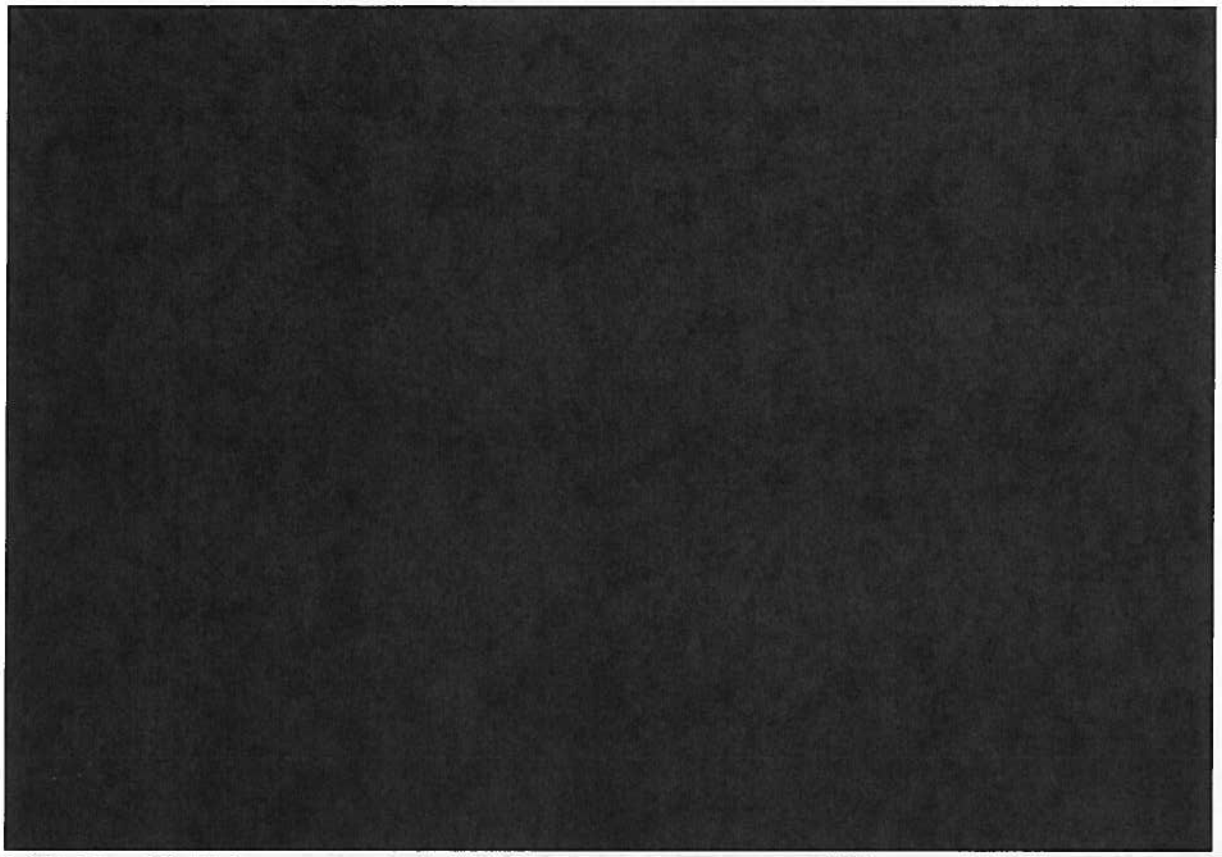
(U) PSP Information	(U) Description of SIGINT Reporting
[redacted]	

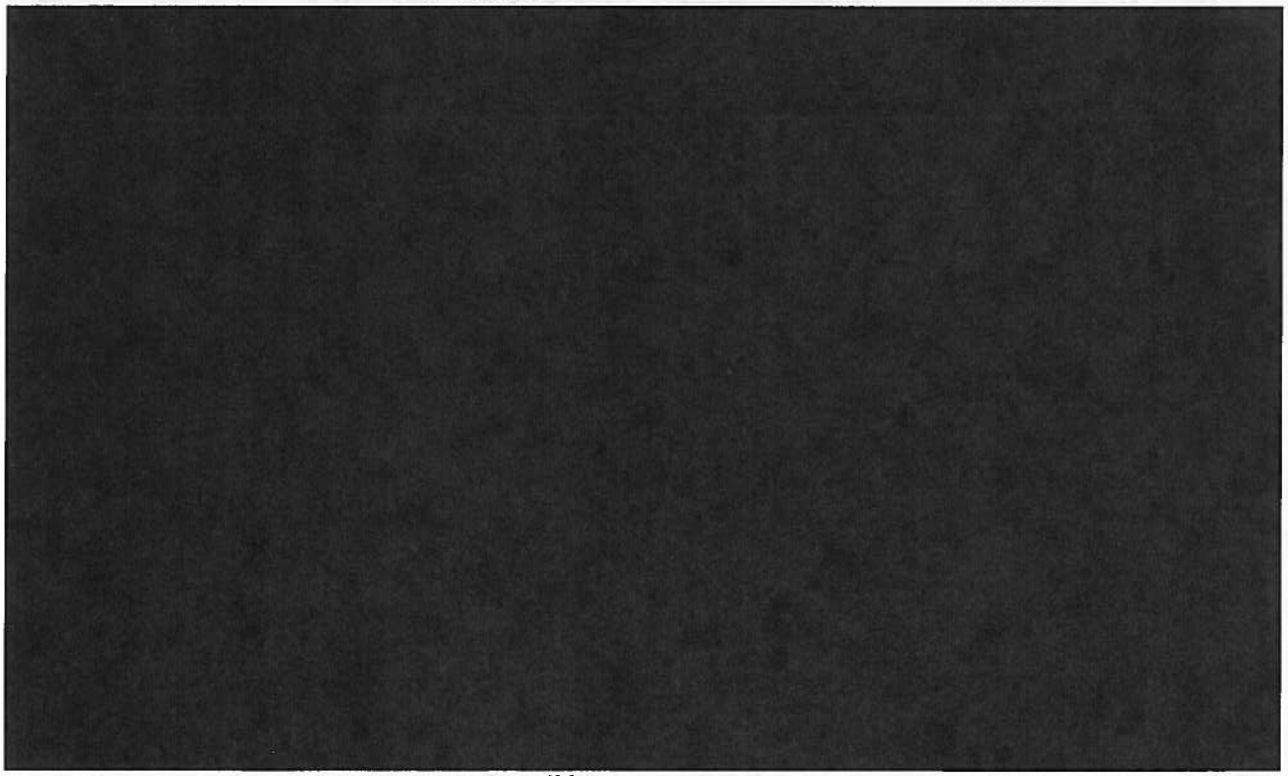
(U) PSP Information	(U) Description of SIGINT Reporting
[redacted]	

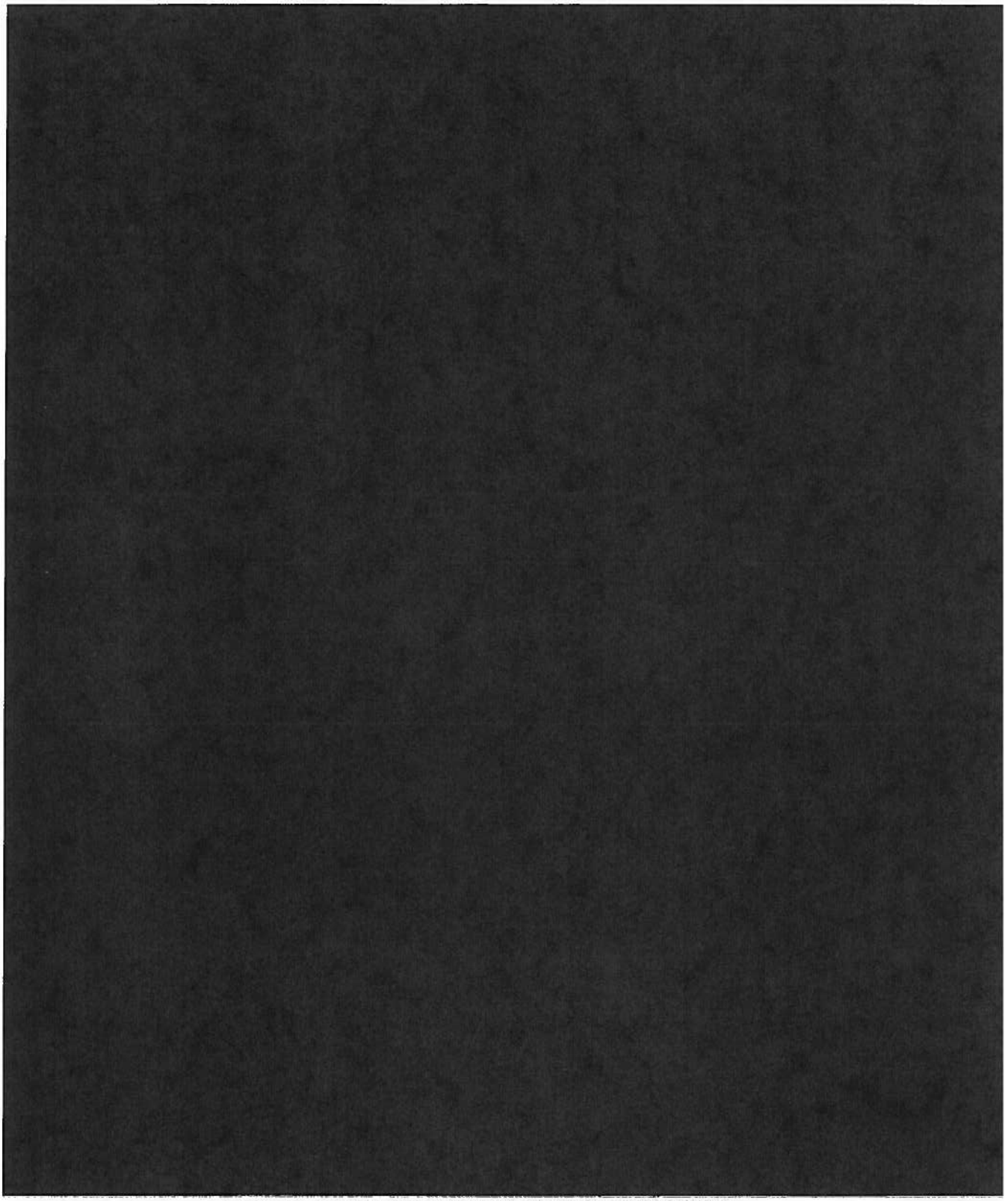
(U) PSP Information	(U) Description of SIGINT Reporting
[redacted]	

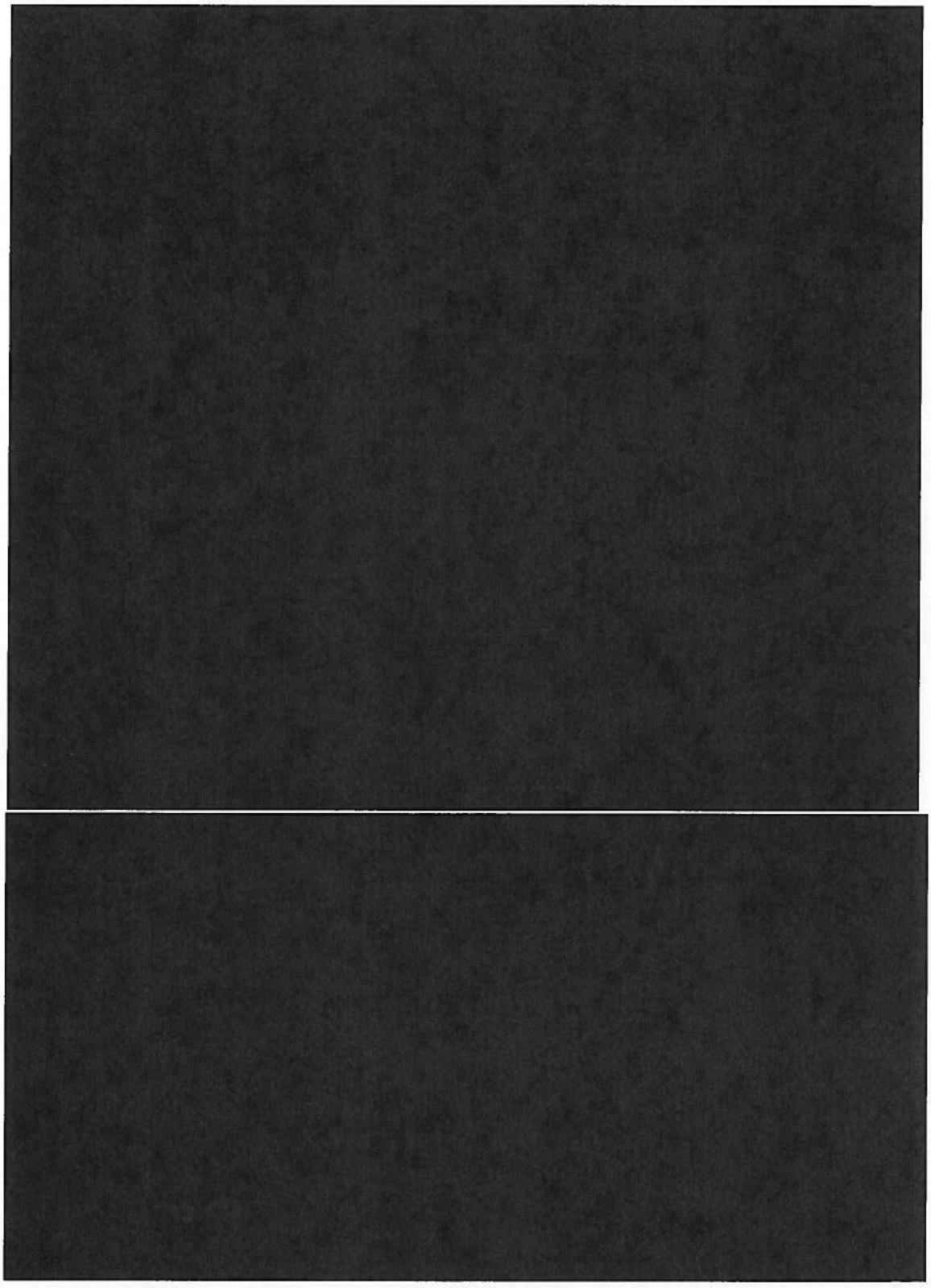
[redacted]

[redacted]

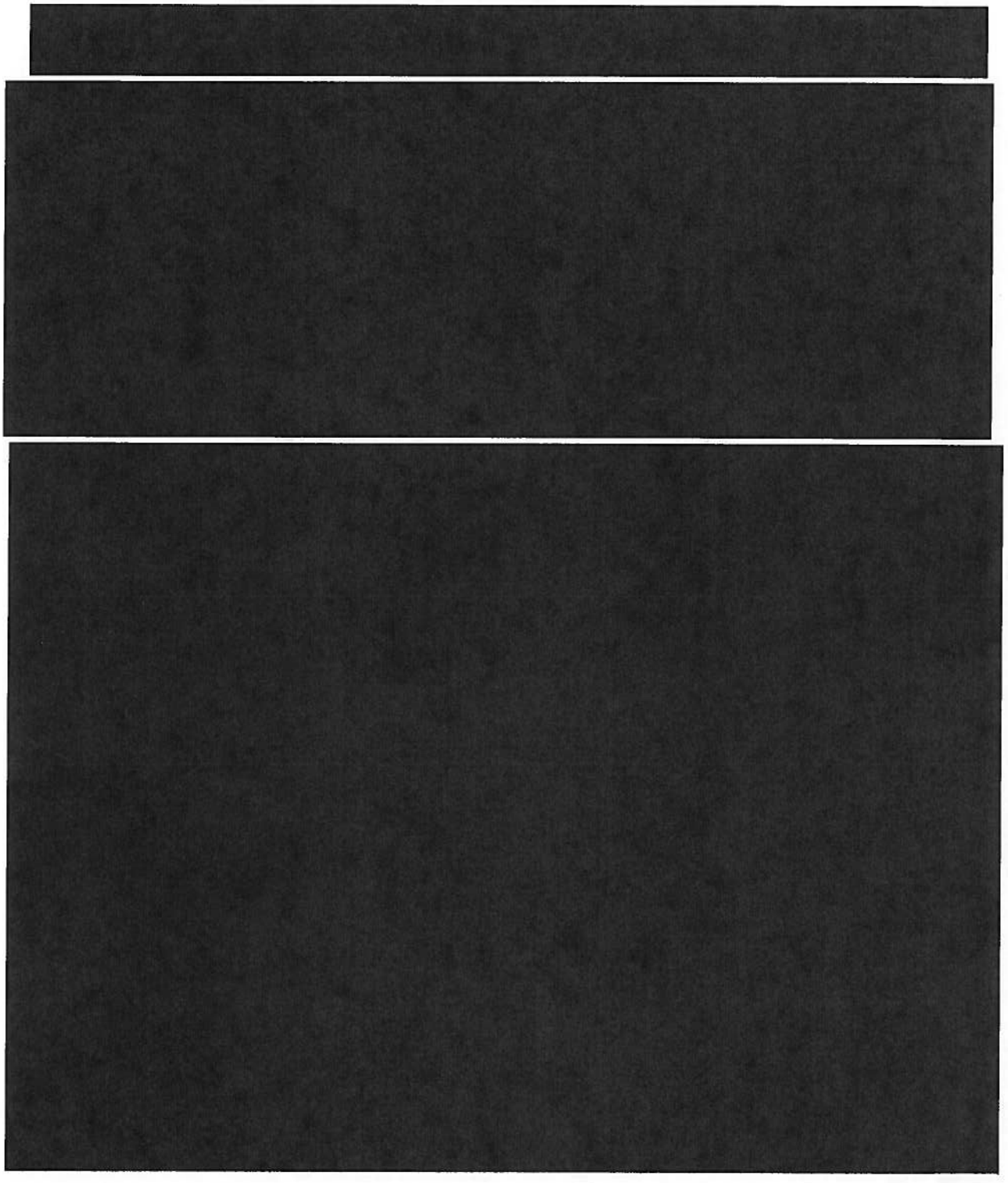






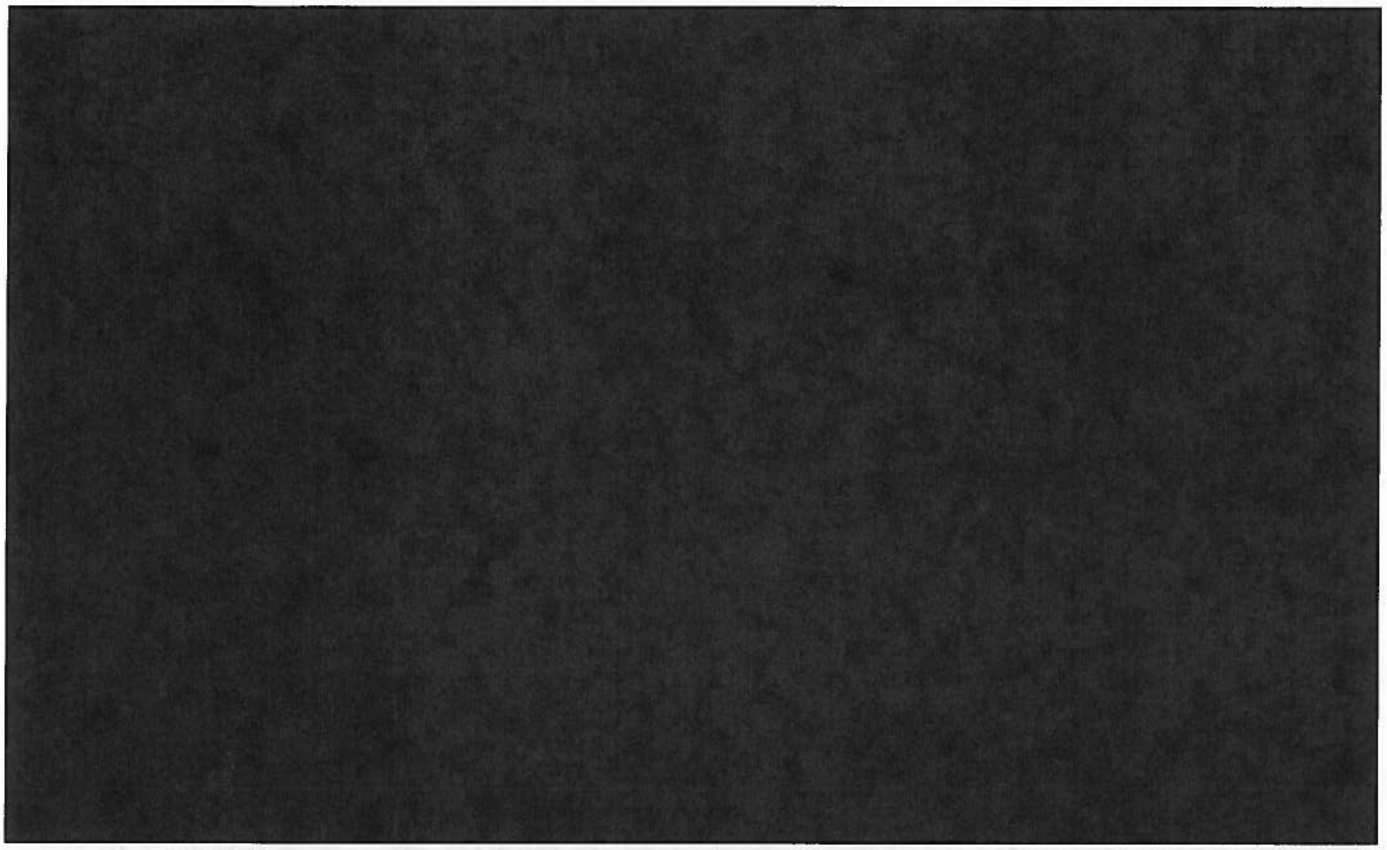


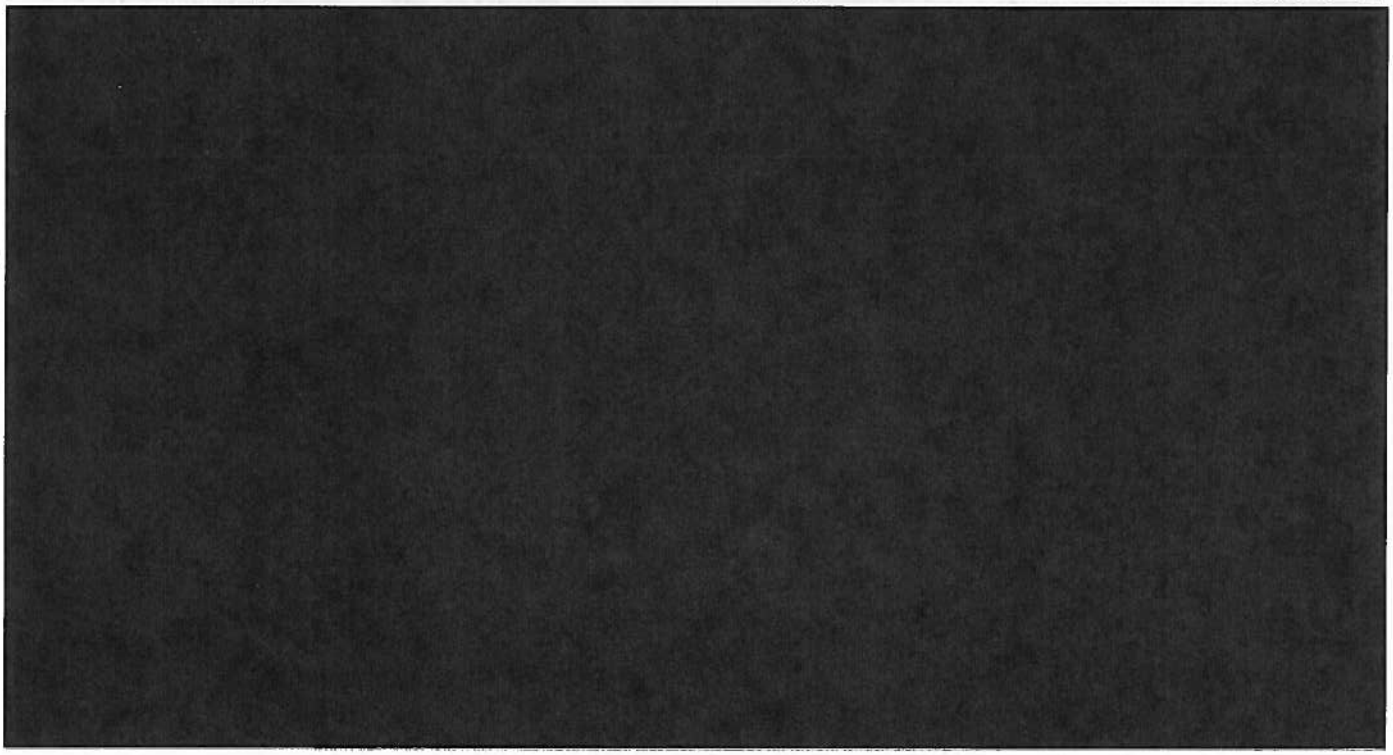
[redacted]



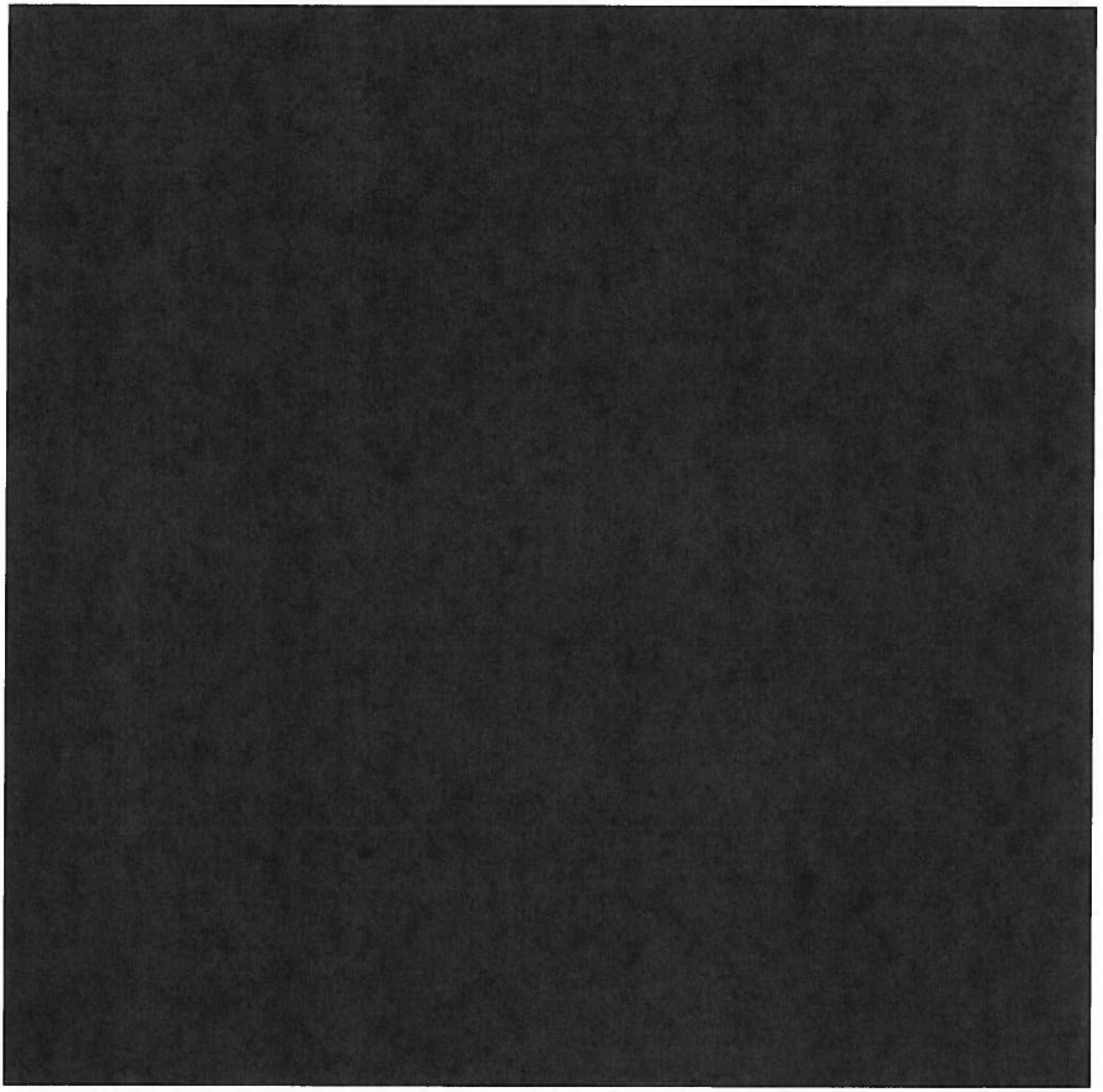
[redacted]

[redacted]

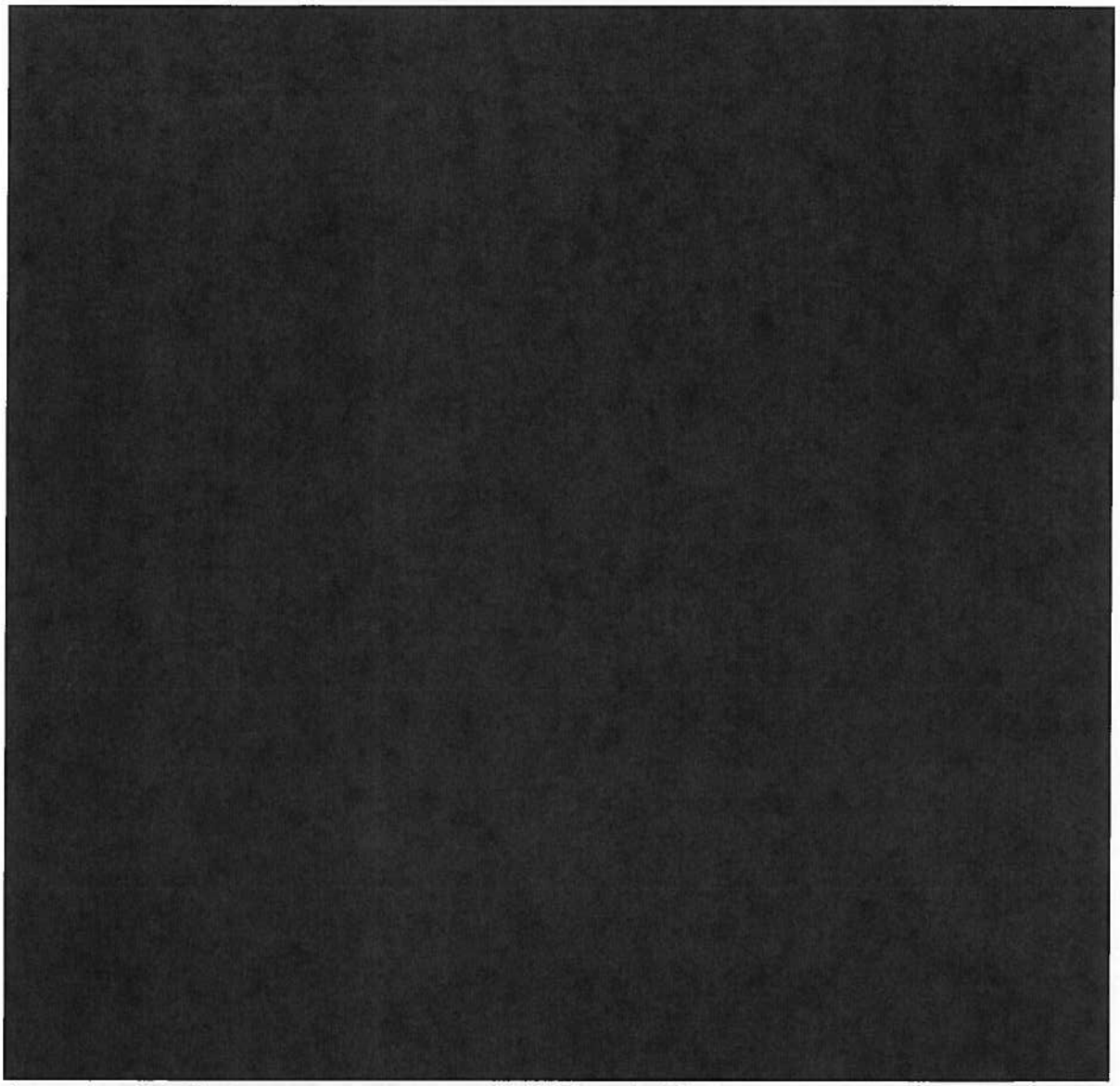


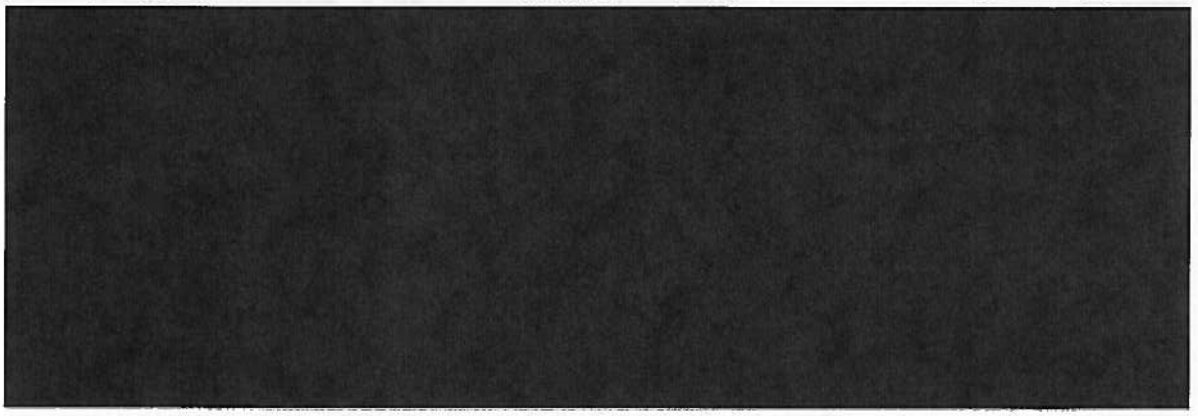


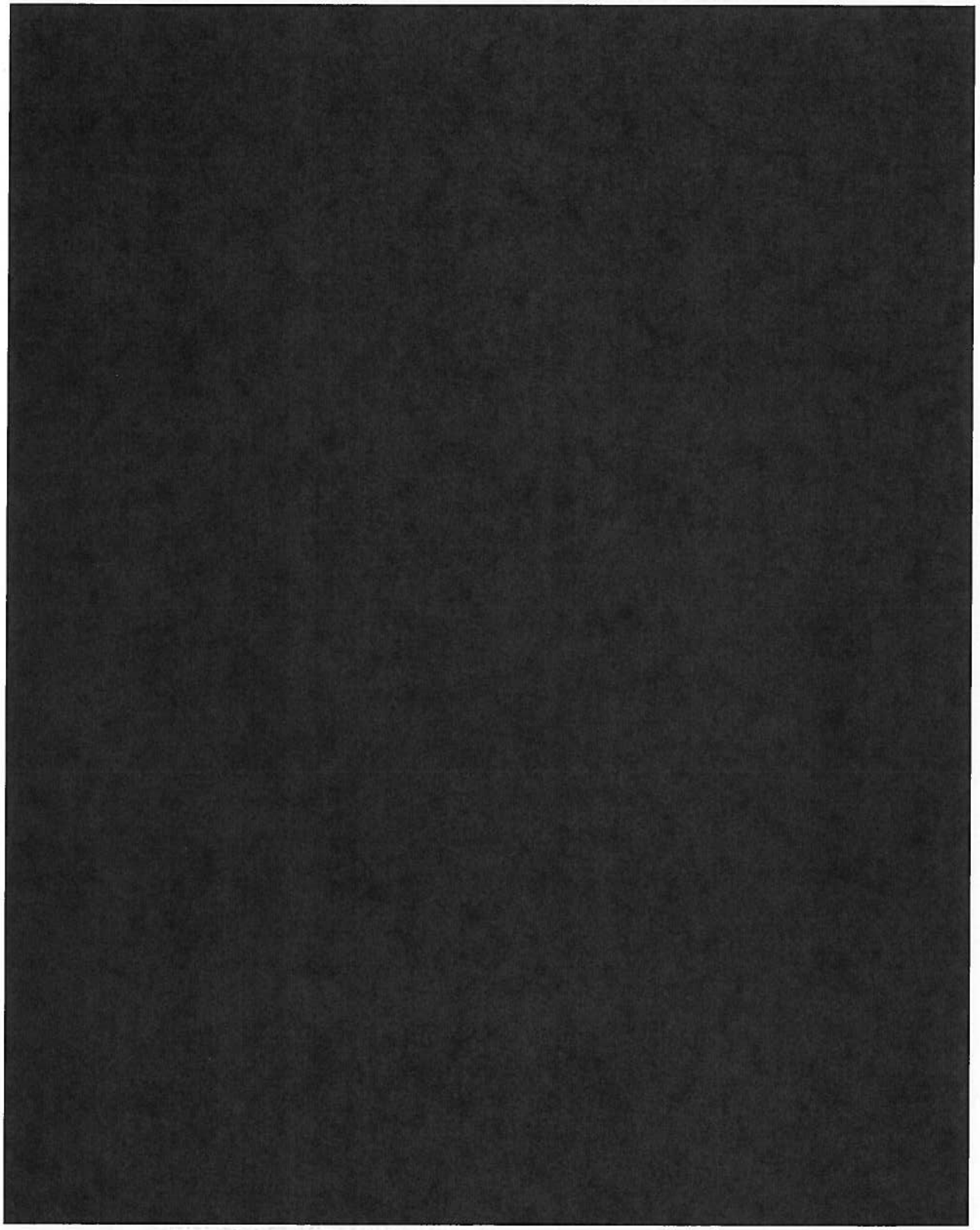
[redacted]

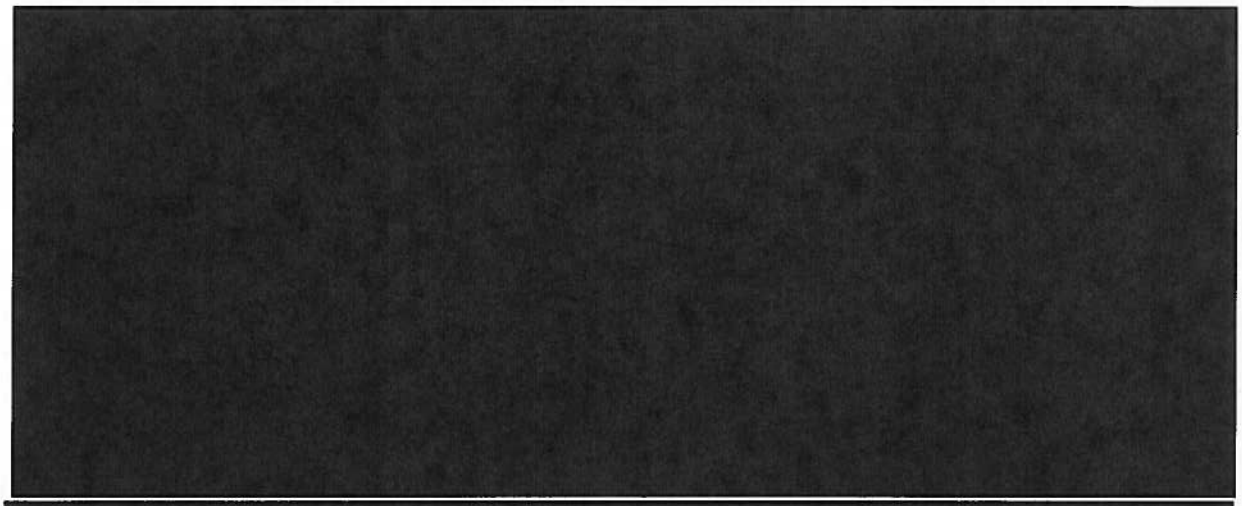


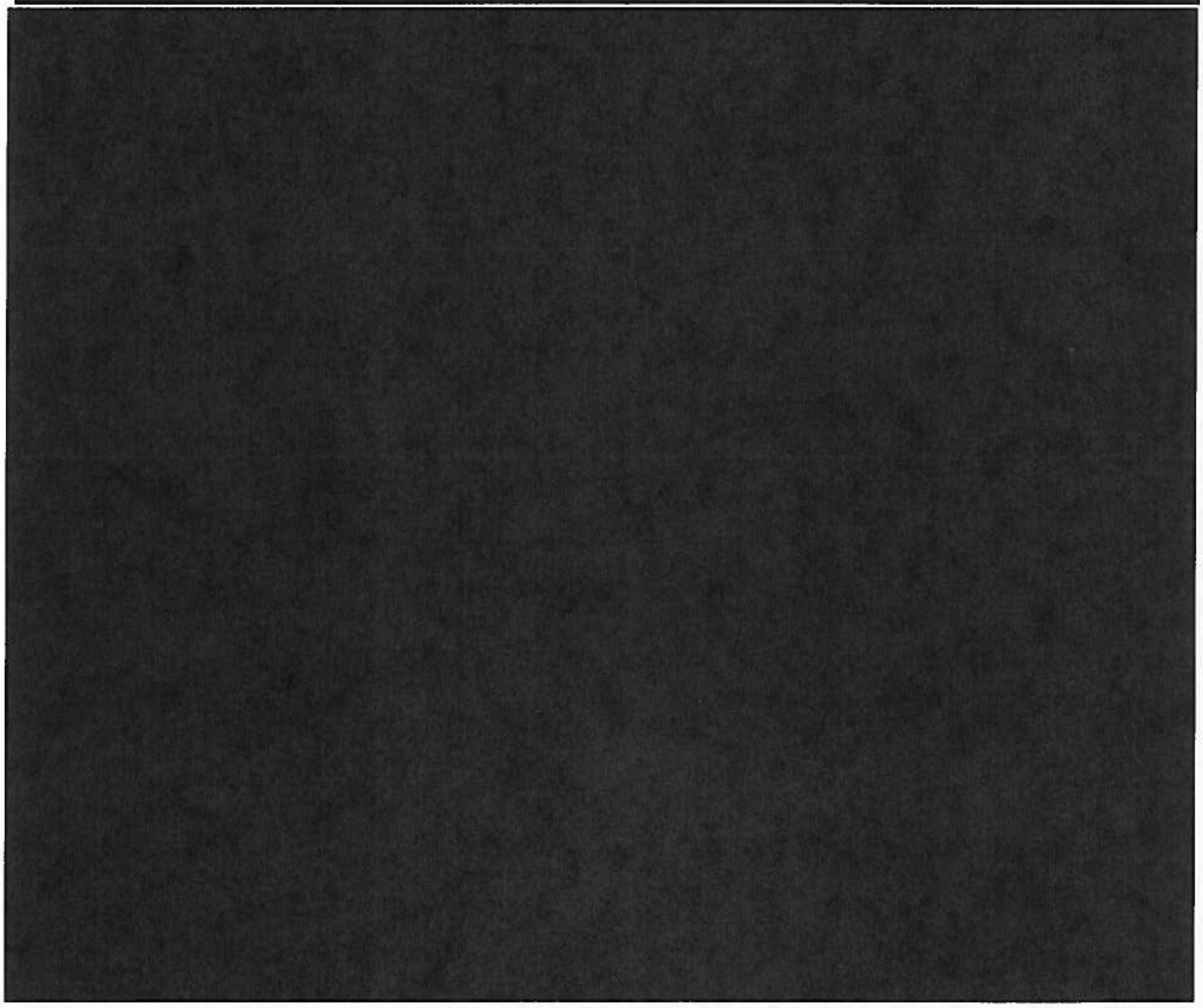
APPROVED FOR PUBLIC RELEASE

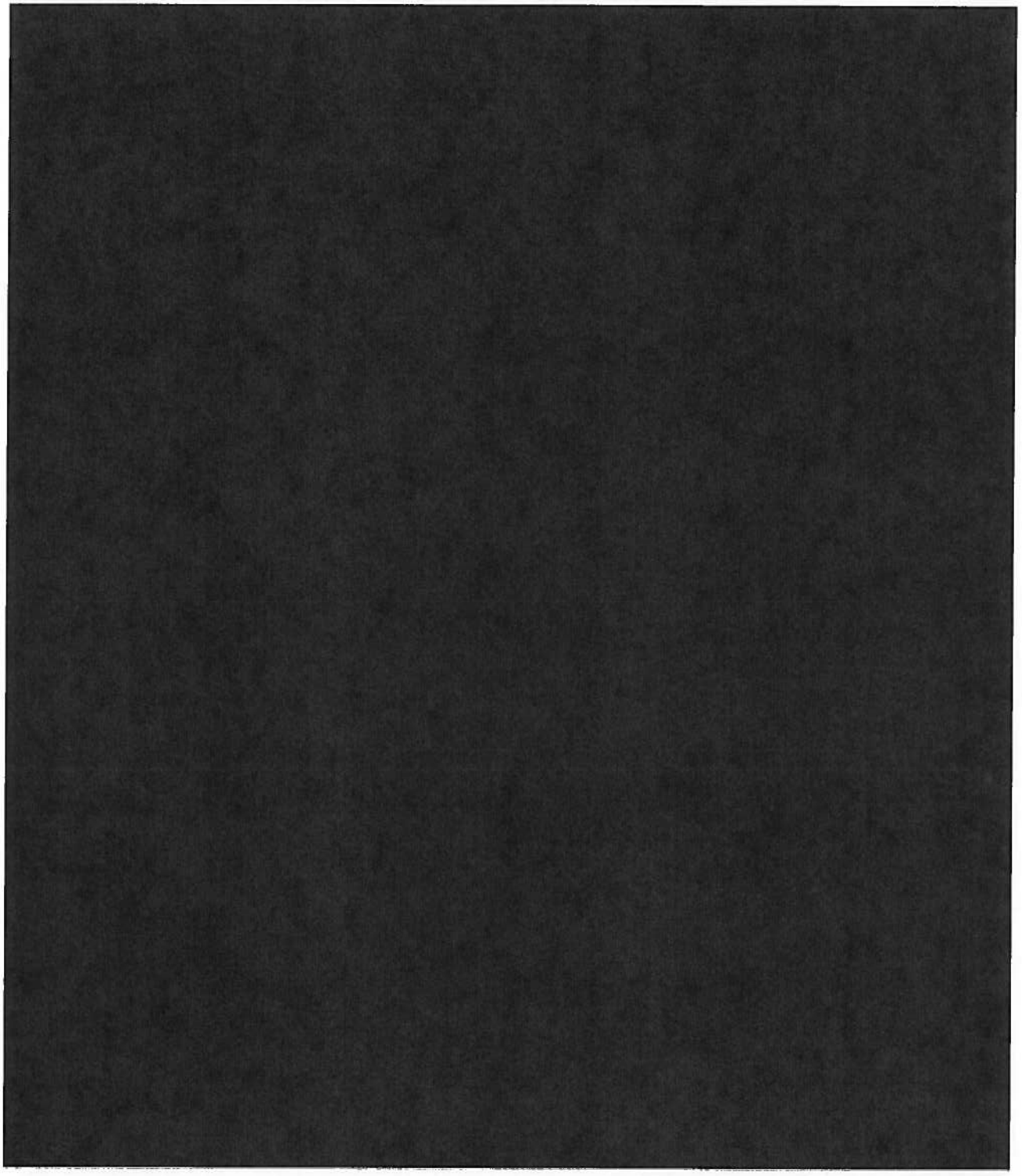




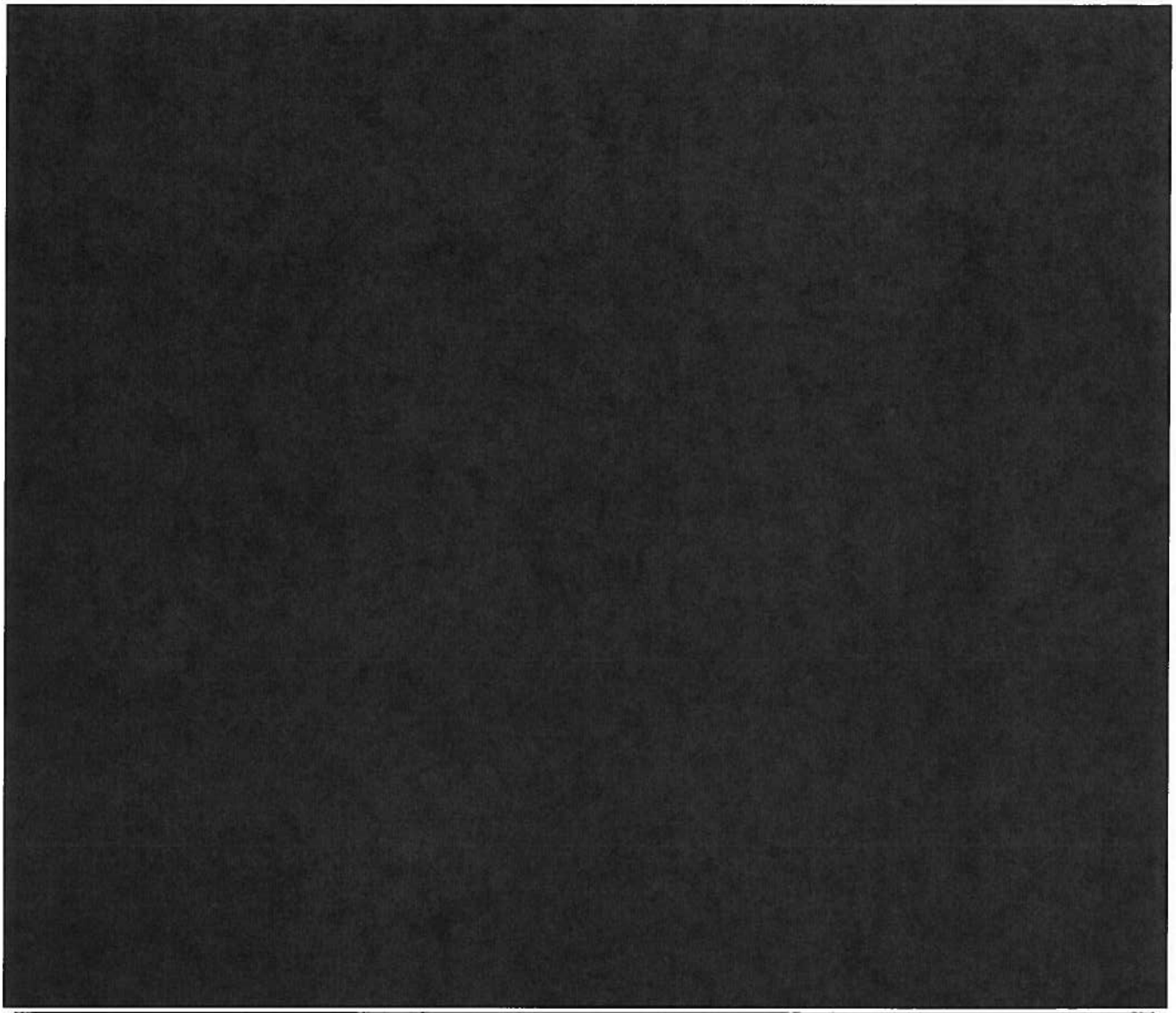


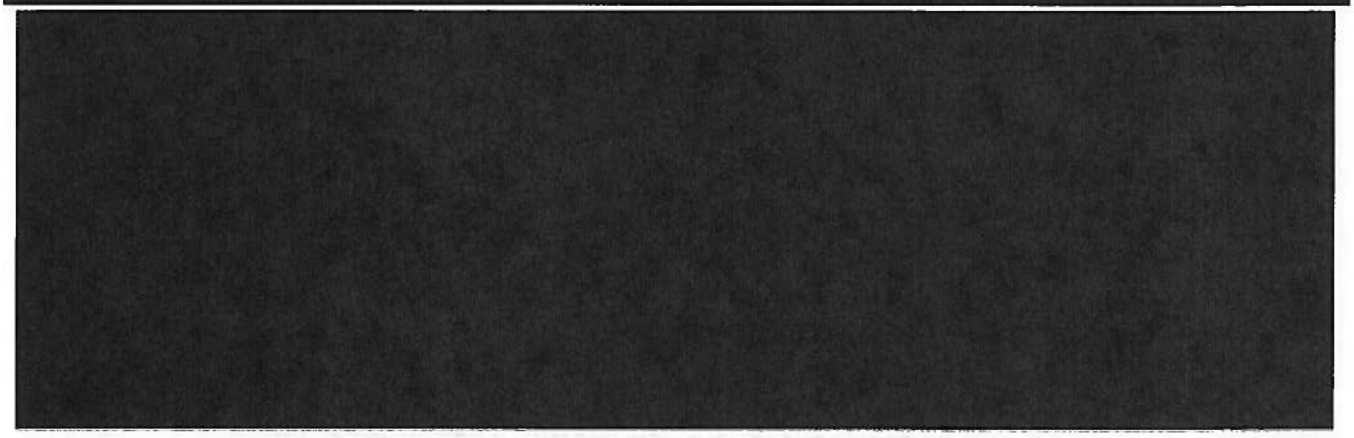






[redacted]



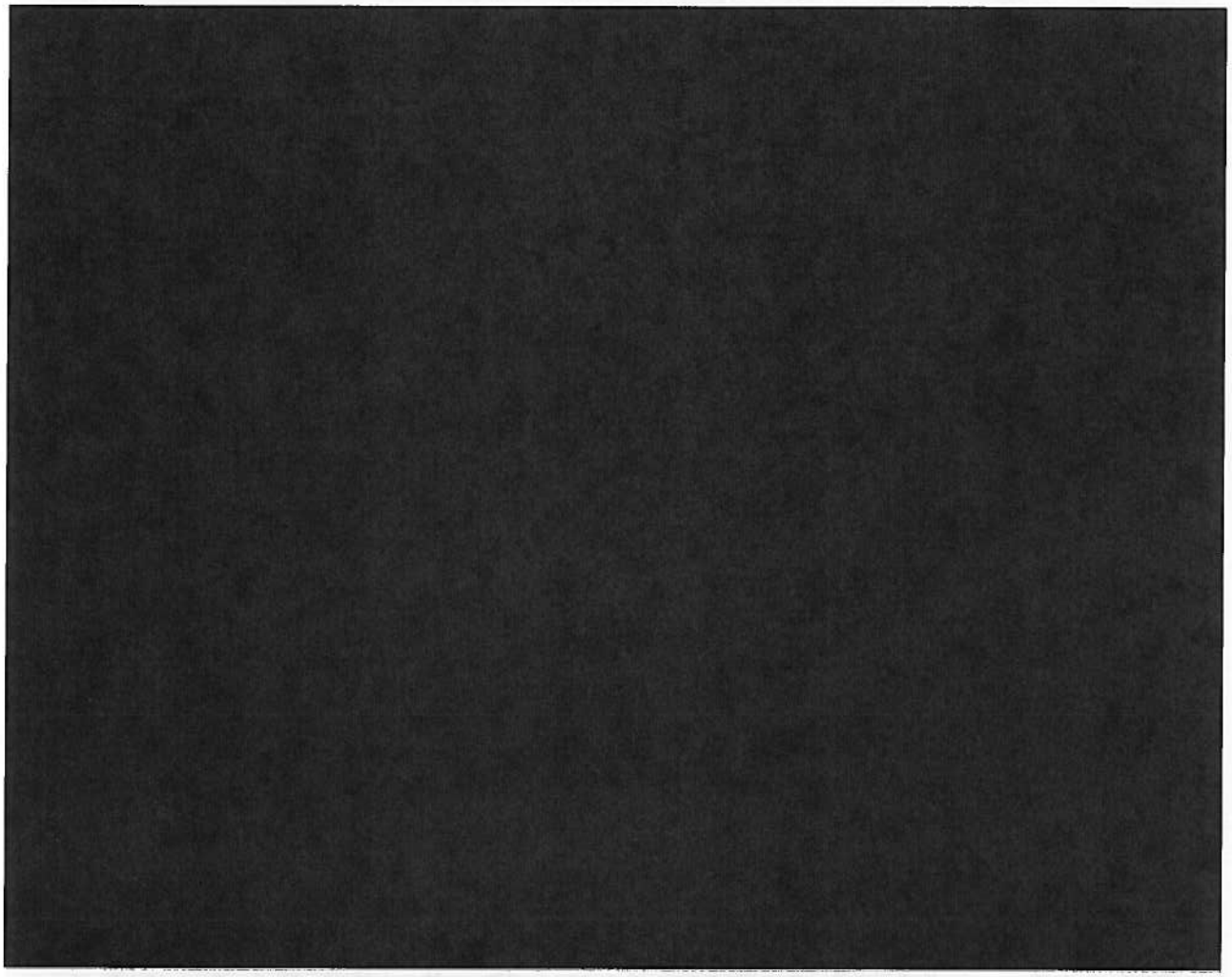


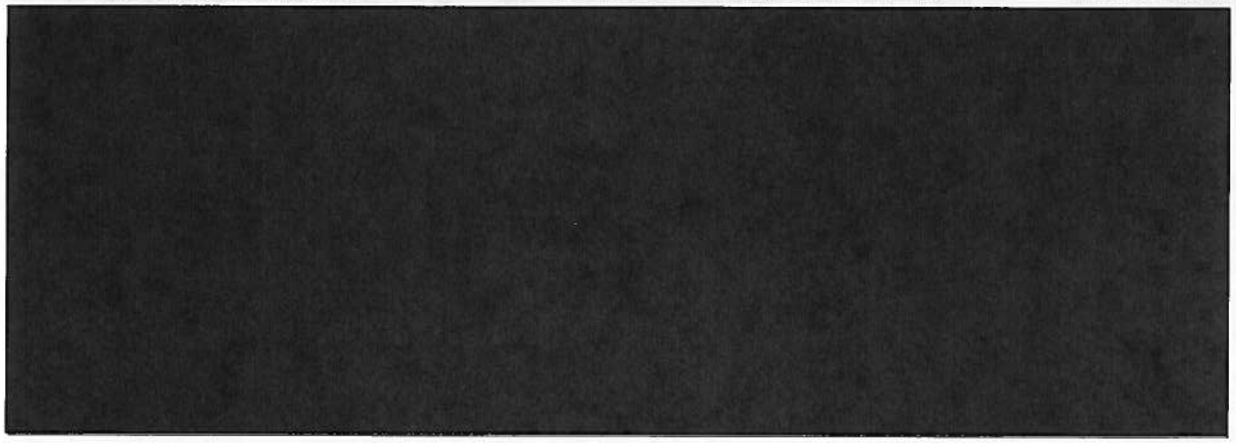
[redacted]

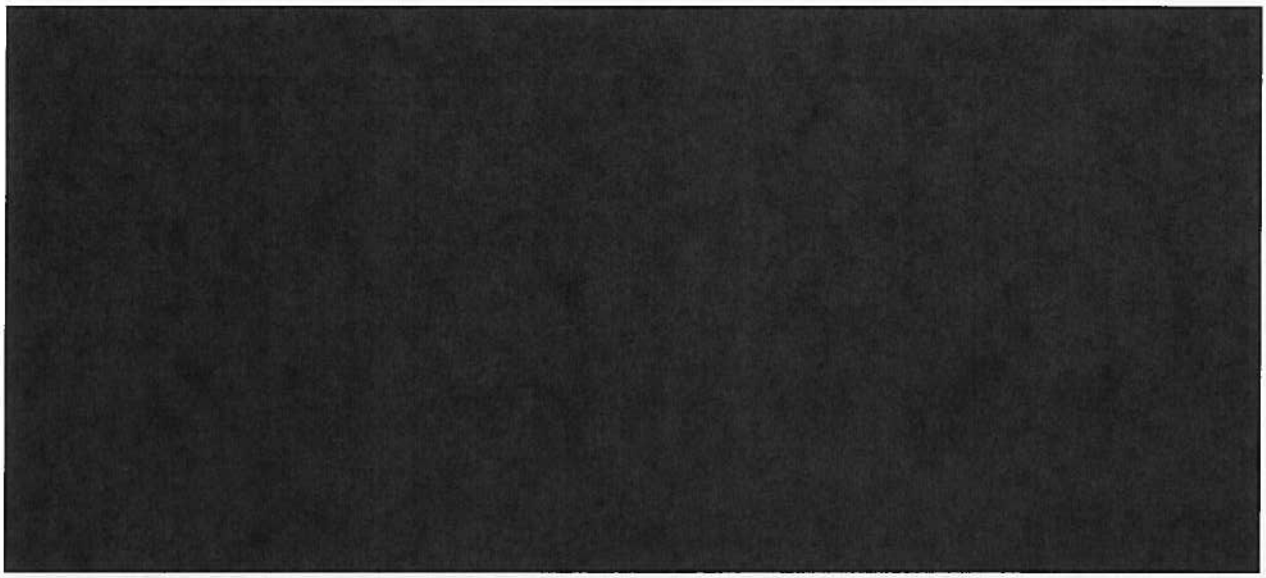
~~(TS//SI//NF)~~ On 12 March, the President directed DoJ to continue working on the legal issues, and on 15 March OLC issued a three page memorandum to the Deputy Attorney General stating that, while it had only begun to analyze the issues and was not yet prepared to issue a final opinion, it believed that [redacted] types of collection authorized under the PSP were legally supportable. OLC had not yet developed a supportable argument to justify [redacted]

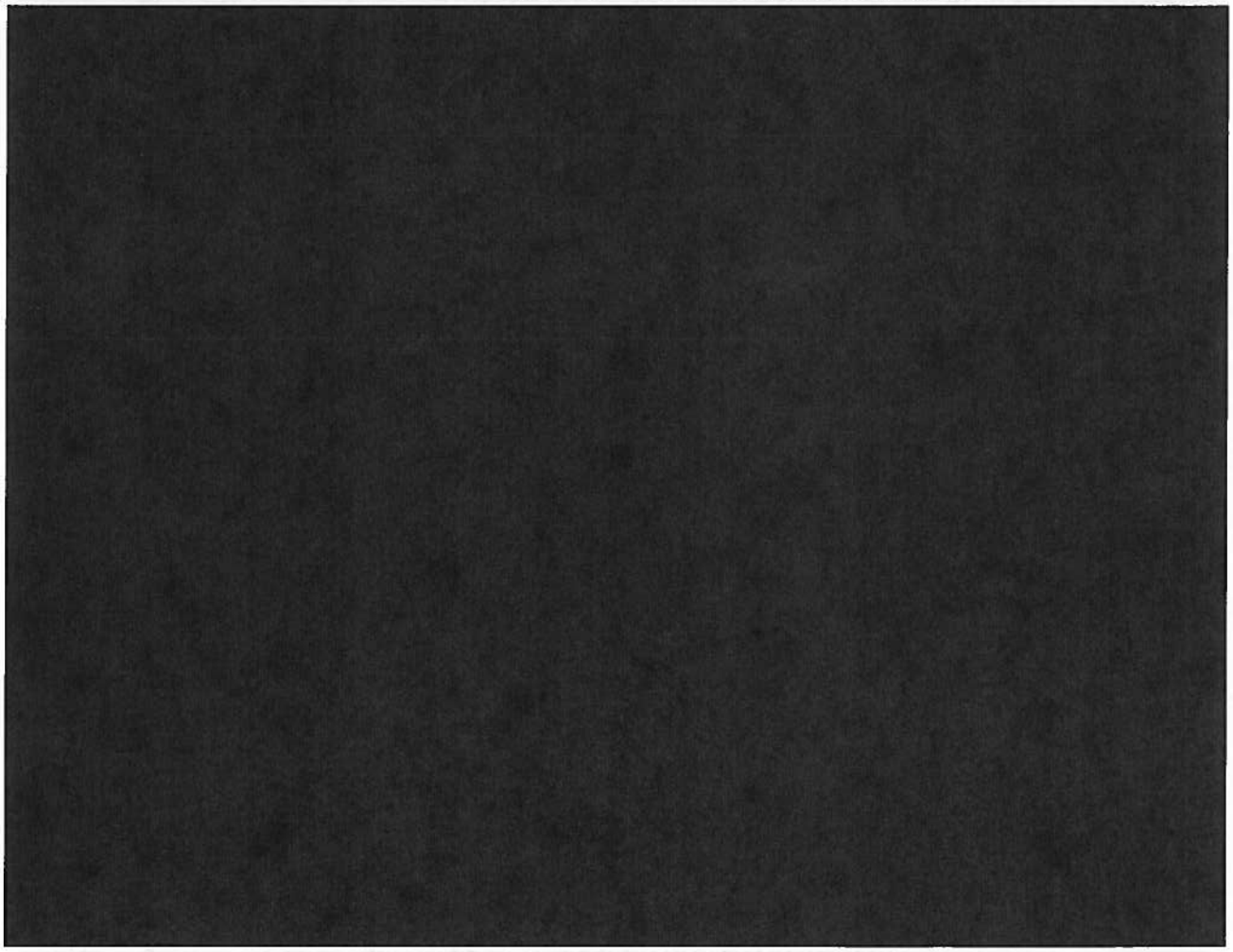
[redacted]

[25] ~~(TS//SI//NF)~~ The Assistant Attorney General for OLC issued a memorandum on 6 May 2004 concluding that operation of the PSP as described in the opinion was lawful. A 16 July memorandum upheld the 6 May opinion [redacted]





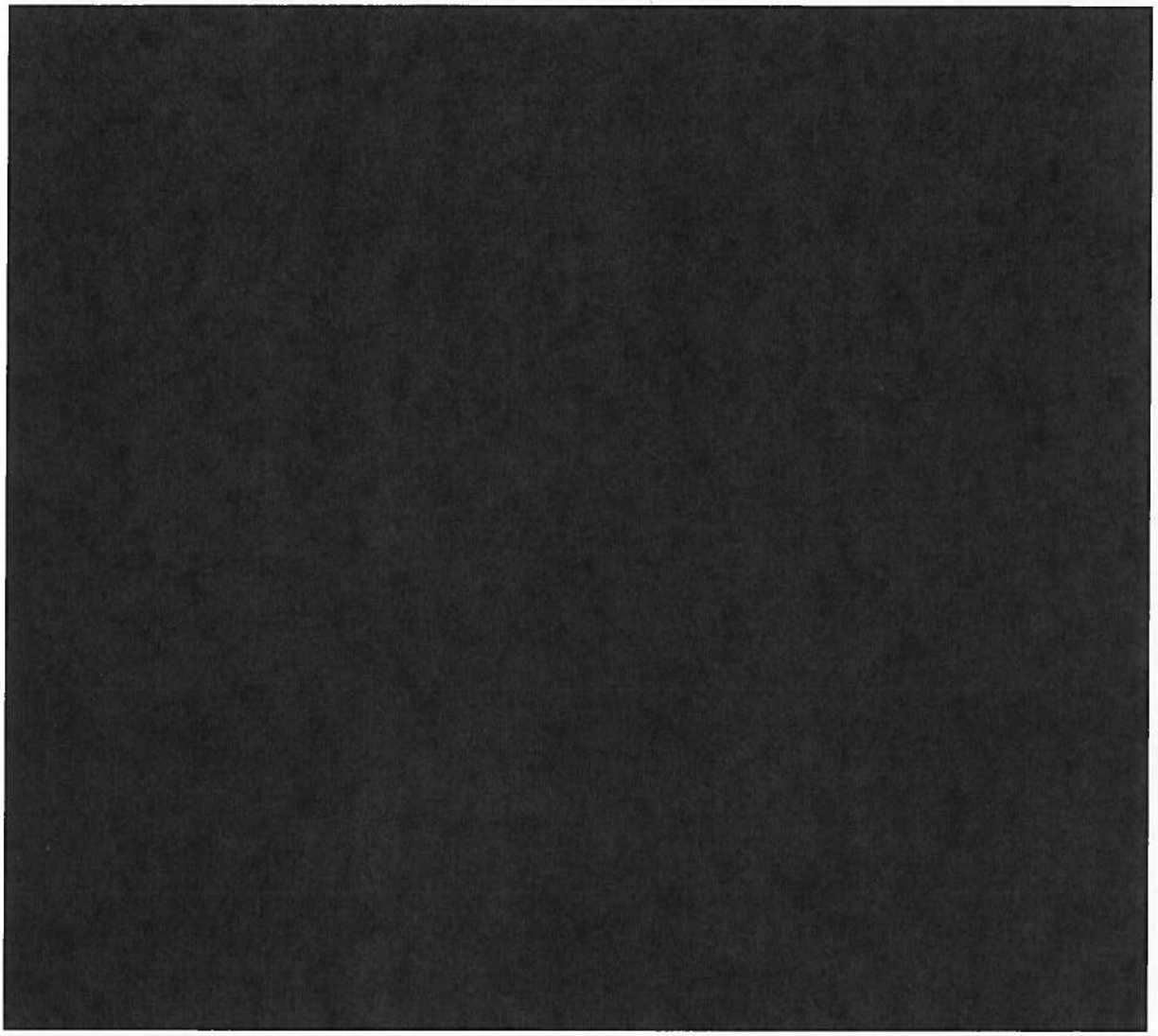




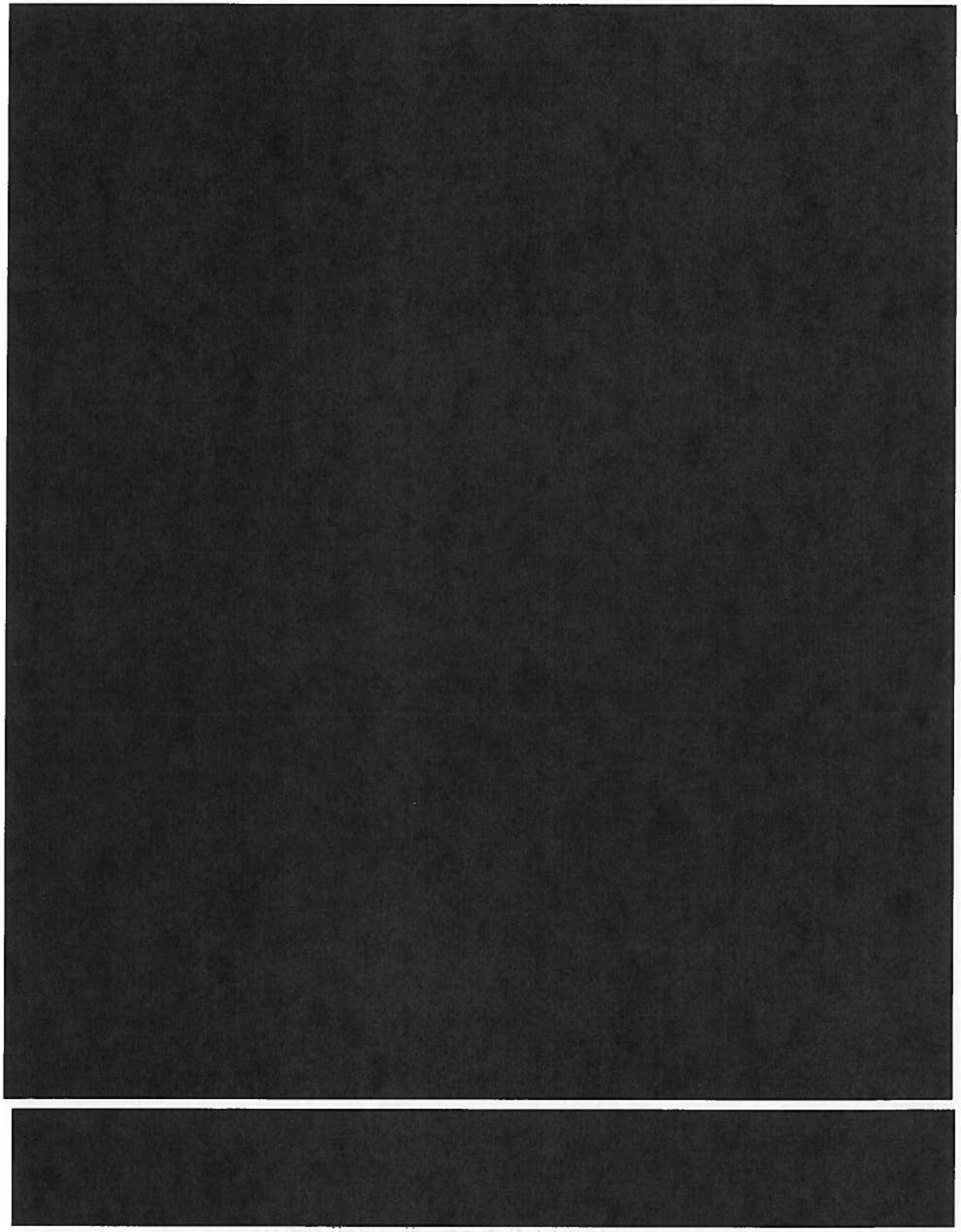
[redacted]

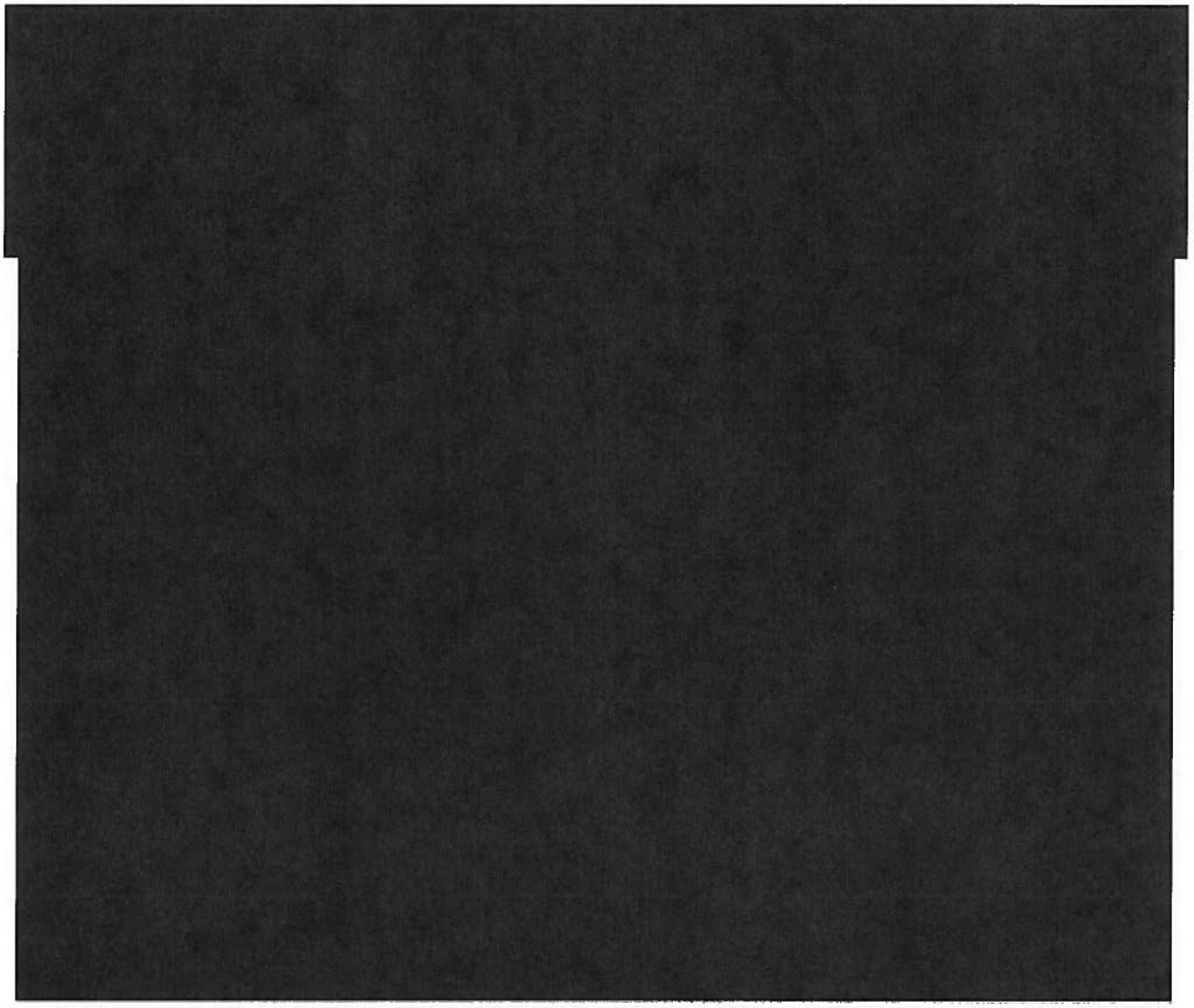
[redacted]

[27] ~~(TS//SI//NF)~~ The minimization probable cause standard states that the Agency may target for collection, communications for which there is probable cause to believe that one of the communicants is a member or agent of [redacted] and the communication is to or from a foreign country.



This page intentionally left blank.





(U//~~FOUO~~) The OIG issued a report for each of the 13 investigations and reviews described above. Ten reports on PSP activity resulted in 11 recommendations to management; 10 have been closed, and one remains open. Three reports on FISC-approved activity previously authorized by the PSP contained nine recommendations to management; three have been closed and six remain open.

~~(TS//STLW//SI//OC/NF)~~ Beginning in January 2007, violations that had occurred under the Authorization and violations related to PSP activity transitioned to court orders were reported quarterly to the President's Intelligence Oversight Board (through the Assistant to the Secretary of Defense for Intelligence Oversight).

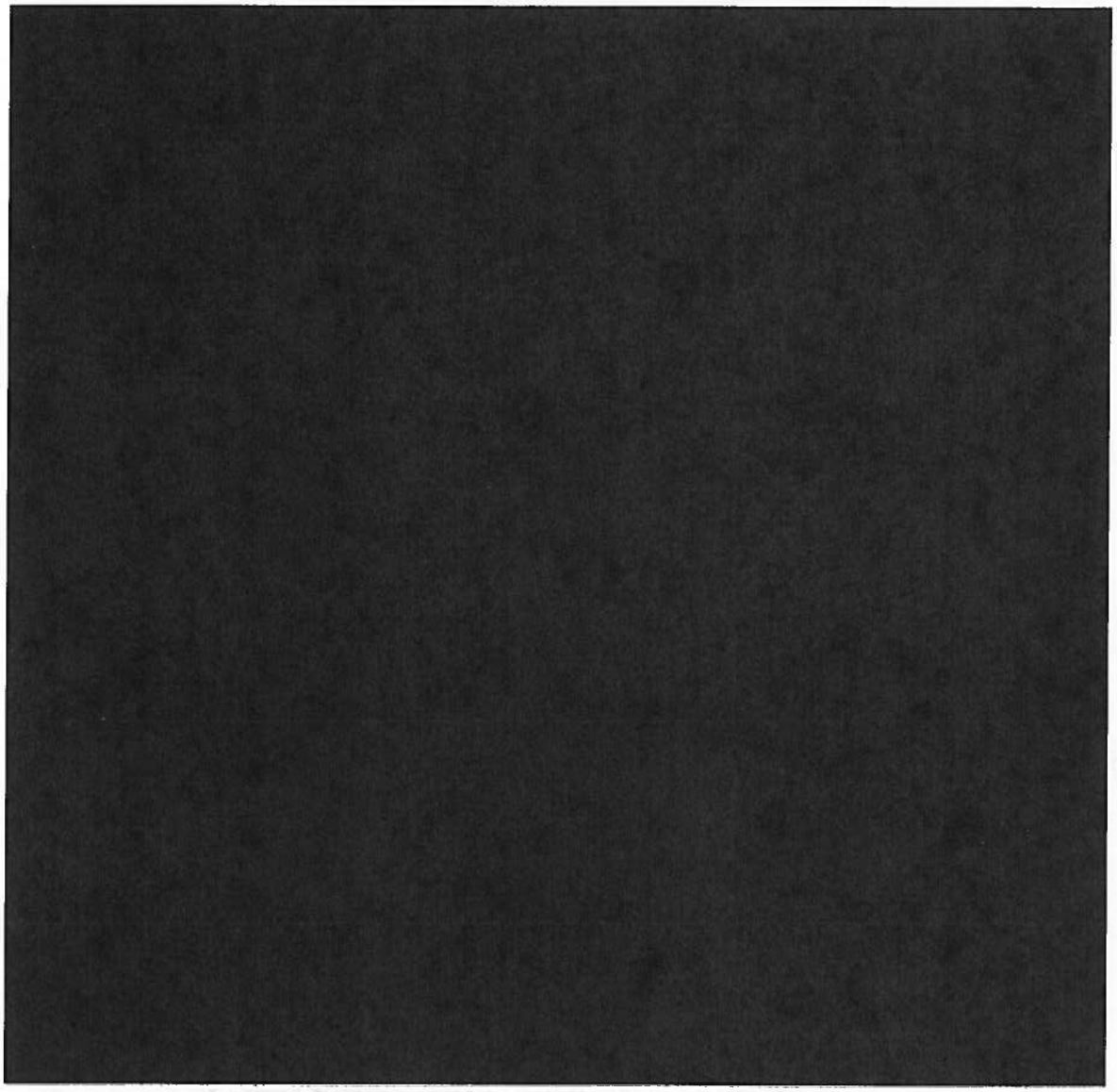
[redacted]

(U) Recently Reported Incidents

~~(TS//STLW//SI//OC/NF)~~ NSA OIG learned in late 2008 that, from approximately [redacted] collection of [redacted] All related records were purged from NSA databases in 2004; therefore, it was not possible to determine the exact nature and extent of that collection. The NSA OIG will close out this incident in an upcoming report to the President's Intelligence Oversight Board.

~~(TS//SI//NF)~~ On 15 January 2009, the Department of Justice reported to the FISC that NSA had been using an "alert list" to compare incoming business records FISA metadata against telephone numbers associated with counterterrorism targets tasked by NSA for SIGINT collection. NSA had reported to the Court that the alert list consisted of numbers for which NSA had determined that a reasonable articulable suspicion existed that the numbers were related to a terrorist organization associated [redacted] However, the majority of selectors on the alert list had not been subjected to a reasonable articulable suspicion determination. The NSA OIG has reported this incident to the President's Intelligence Oversight Board and has filed updates as required. The alert list and a detailed NSA 60-day review of processes related to the Business Records FISC order were the subject of several recent submissions to the FISC and of NSA briefings to Congressional oversight committees.

[redacted]



(U//~~FOUO~~) Other IG Program concerns were documented in the 2003-2008 reports. Presidential Notifications are listed and described in Appendix F. The 2008 report described the adequacy of Program decompartmentation plans.

(U) ACRONYMS AND ABBREVIATIONS

~~(TS//SI//NF)~~

Bps	Bits per Second
BR	Business Records
CDR	Call Detail Records
[redacted]	
CIA	Central Intelligence Agency
COMINT	Communications Intelligence
CT	Counterterrorism
DCI	Director of Central Intelligence
DNI	Director of National Intelligence
DoD	Department of Defense
DoJ	Department of Justice
EO	Executive Order
FAA	FISA Amendments Act
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
GC	General Counsel
Gbps	Gigabits per Second
HPSCI	House Permanent Select Committee on Intelligence
IG	Inspector General
LAN	Local Area Network
[redacted]	[redacted]
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
O&C	Oversight and Compliance
ODNI	Office of the Director of National Intelligence
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OIPR	Office of Intelligence Policy and Review (now the Office of Intelligence, National Security Division)
OLC	Office of Legal Counsel

PM	Program Manager
PR/TT	Pen Register/Trap & Trace
PSP	President's Surveillance Program
RFI	Request for Information
SID	Signals Intelligence Directorate
SIGINT	Signals Intelligence
SSCI	Senate Select Committee on Intelligence
[redacted]	
TS/SCI	Top Secret/Sensitive Compartmented Information

~~(TS//SI//NF)~~

(U) GLOSSARY OF TERMS

(U) COMINT	(U) Communications Intelligence – technical and intelligence information derived from foreign communications by someone other than the intended recipients
(U) E.O. 12333	(U) Executive Order 12333 - *United States Intelligence Activities* - provides goals, duties, and responsibilities with respect to the national intelligence effort. It mandates that certain activities of U.S. intelligence components are to be governed by procedures issued by agency heads and approved by the Attorney General.
(U) FISA	(U) The Foreign Intelligence Surveillance Act of 1978, as amended, governs the conduct of certain electronic surveillance activities within the United States to collect foreign intelligence information.
(U) [redacted]	~~(S//SI//NF)~~ Analytic tool for contact chaining used by analysts to do target discovery by quickly and easily navigating global communications metadata
~~(TS//SI//NF)~~ METADATA	~~(TS//SI//NF)~~ Header, router, and addressing-type information, including telecommunications dialing-type data, but not the contents of the communication
(U) [redacted]	[redacted]
(U) [redacted]	~~(S//NF)~~ NSA's primary storage, search, and retrieval mechanism for SIGINT text
(U) SANITIZATION	(U) The process of disguising COMINT to protect sensitive intelligence sources, methods, capabilities, and analytical procedures in order to disseminate the information outside COMINT channels.

(U) SIGNALS INTELLIGENCE	(U) A category of intelligence comprising individually or in combination all communications intelligence (COMINT), electronic intelligence (ELINT) and foreign instrumentation intelligence (FISINT), however transmitted.
(U) TEAR LINE REPORTS	(U) Reports used to disseminate SIGINT-derived information and sanitized information in the same record. The sanitized tear line conveys the same facts as the COMINT-controlled information, while hiding COMINT as the source.
(U) TELEPHONY	(U) The technology associated with the electronic transmission of voice, fax, and other information between parties using systems historically associated with the telephone
(U) TIPPERS	[redacted]

APPENDIX A

(U) About the Review

This page intentionally left blank.

(U) About the Review

(U) Objectives

(U) The Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, which was signed into law on 10 July 2008, requires that the Inspectors General of Intelligence Community elements that participated in the President's Surveillance Program (PSP) conduct a comprehensive review of the Program. The NSA Office of the Inspector General (OIG) reviewed NSA's participation in the PSP. The specific review objectives were to examine:

- (U) The establishment and evolution of the PSP as it affected NSA
- (U) NSA implementation of the PSP, including preparation and dissemination of product under the PSP
- (U) NSA access to legal reviews of the PSP and access to information about the Program
- (U) NSA communications with and representations made to private sector entities and private sector participation
- (U) NSA interaction with the Foreign Intelligence Surveillance Court (FISC) and transition of PSP-authorized collection to court orders
- (U) Oversight of PSP activities at NSA.

(U) Scope and Methodology

(U) This review was conducted in accordance with generally accepted government auditing standards, as set forth by the Comptroller General of the United States and implemented by the audit manuals of the DoD and NSA/CSS Inspectors General.

(U) The review was conducted from 10 July 2008 to 15 May 2009 in coordination with the Inspectors General of the Department of Defense, Office of the Director of National Intelligence, CIA, and DoJ.

(U//~~FOUO~~) The scope of this review was limited to NSA's participation in the PSP from 4 October 2001 to 17 January 2007. The review included NSA activities before and after the terrorist attacks of 11 September 2001 that led to the Presidential Authorization on 4 October 2001. It also included the transition of PSP-authorized activity to FISC orders.

~~(TS//NF)~~ To satisfy review objectives, we interviewed [redacted] current and former NSA personnel who participated in the PSP including NSA Directors and Deputy Director, General Counsels, Deputy General Counsels, Associate General Counsels for Operations, and the Inspector General responsible for Program oversight from August 2002 until August 2006. We also interviewed former [redacted] as well as leadership [redacted] within the Signals Intelligence Directorate.

~~(TS//SI//NF)~~ Interviews of the former Director of NSA, General Hayden, the former NSA Associate General Counsel for Operations, [redacted] were conducted with other IG offices involved in the joint PSP review.

(U//~~FOUO~~) We requested White House documentation of meetings at which General Hayden or NSA employees discussed the PSP or the Terrorist Surveillance Program with the President, Vice President, or White House personnel, but did not receive a response before publication of this report.

~~(TS//SI//NF)~~ [redacted]

(U//~~FOUO~~) We reviewed NSA records dated 27 July 1993 to 10 July 2008 that pertained to review objectives. Records included NSA policies and regulations, correspondence, e-mail, briefings, notes, reports, calendars, and database reports.

~~(S//NF)~~ Numbers of selectors tasked and reports issued were based on information provided by the PSP Program Management Office and were not independently verified during this review.

(U//~~FOUO~~) Information about individuals cleared for access to Program information was based on records provided by the PSP Project Security Officer and were not independently verified during this review.

(U) Prior Coverage

(U//~~FOUO~~) The OIG began oversight of the PSP and related activities in August 2002 and issued twelve reports dated 21 February 2003 through 30 June 2008 (Appendix E.) The OIG also issued 14 Presidential notifications from March 2003 to October 2006 (Appendix F). Detailed discussion of the OIG's oversight of the PSP is included in Section VIII of this report.

~~(TS//SI//NF)~~ As portions of the Program were transitioned to FISC orders for the collection of internet metadata and telephony business records, the OIG reviewed the execution and adequacy of controls in ensuring compliance with the orders. The OIG did not test the efficacy of controls for metadata collected under the authority of the PSP or court orders. Three reports summarized OIG investigations into possible misuse of the Authority or violations of FISC orders. One report summarized the OIG's oversight of the PSP, and the last report reviewed the adequacy of Program decompartmentation plans.

This page intentionally left blank.

APPENDIX B

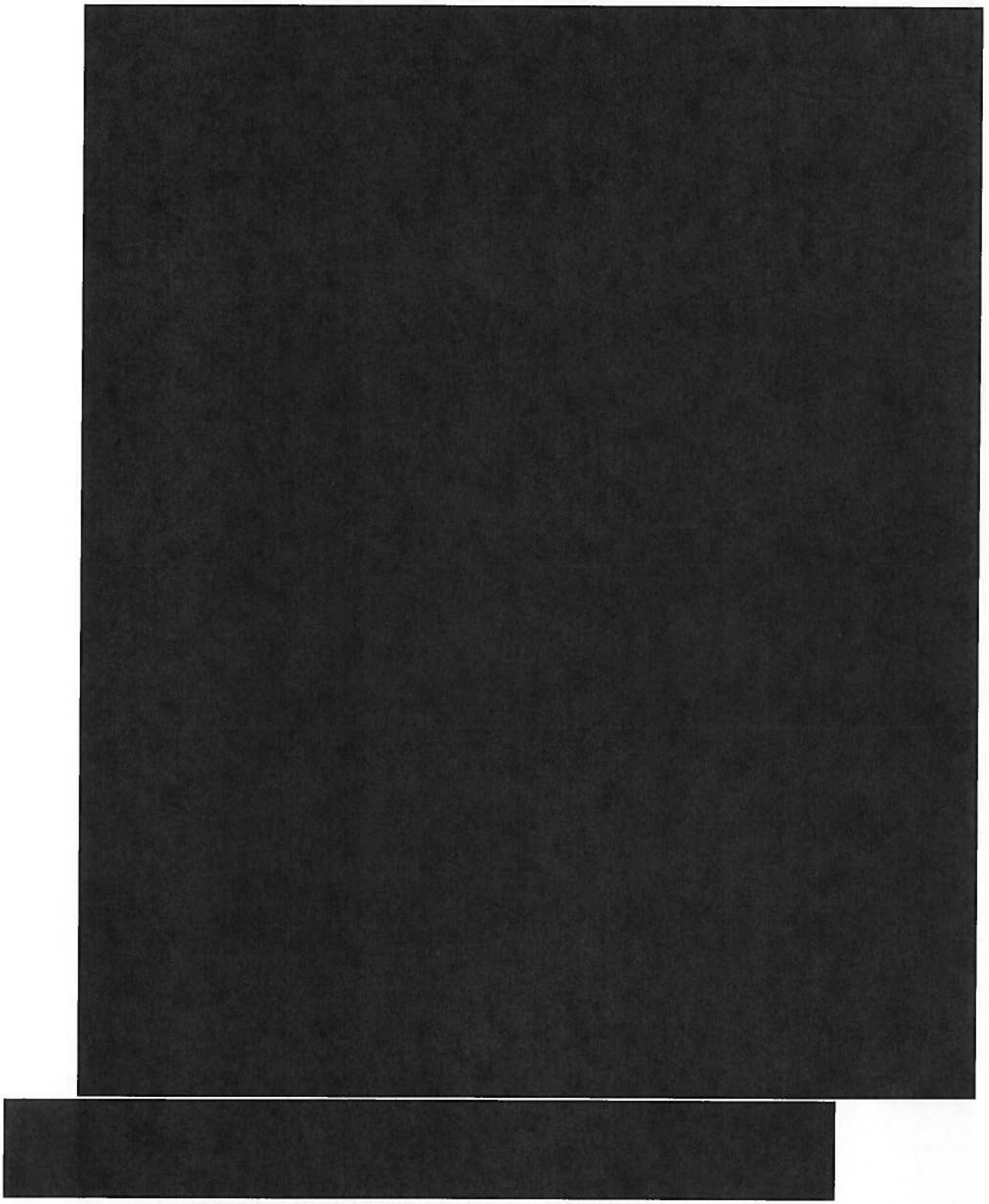
(U) The Presidential Authorizations

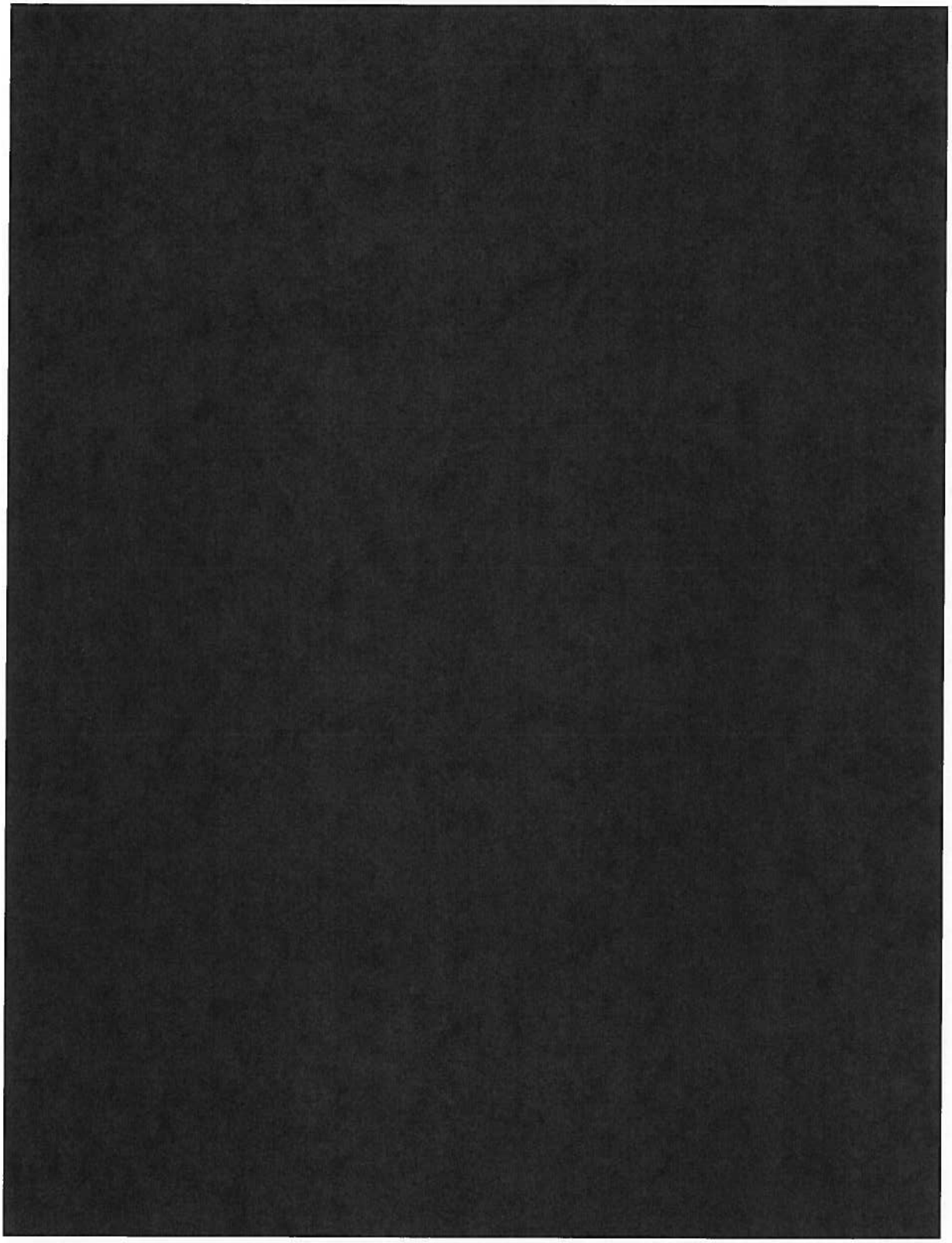
This page intentionally left blank.

(U) The Presidential Authorizations

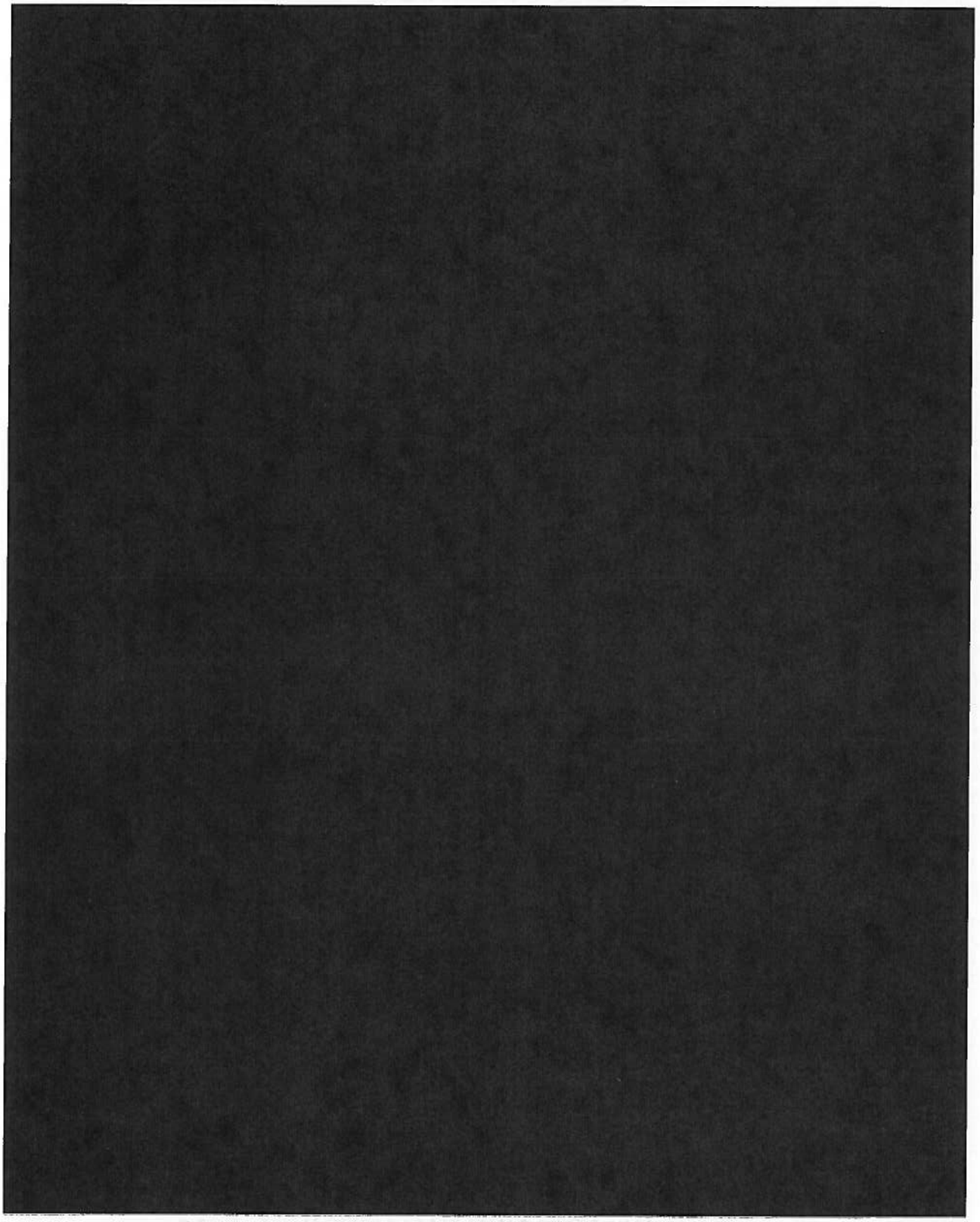
~~(TS//STLW//SI//OC/NF)~~ The Authorization documents that contained the terms under which NSA executed special Presidential authority were addressed to the Secretary of Defense and were titled "*Presidential Authorization for Specified Electronic Surveillance Activities during a Limited Period to Detect and Prevent Acts of Terrorism within the United States.*" The first Authorization consisted of [redacted] There were 43 Authorizations, two modifications, and one document described as [redacted]

[redacted]

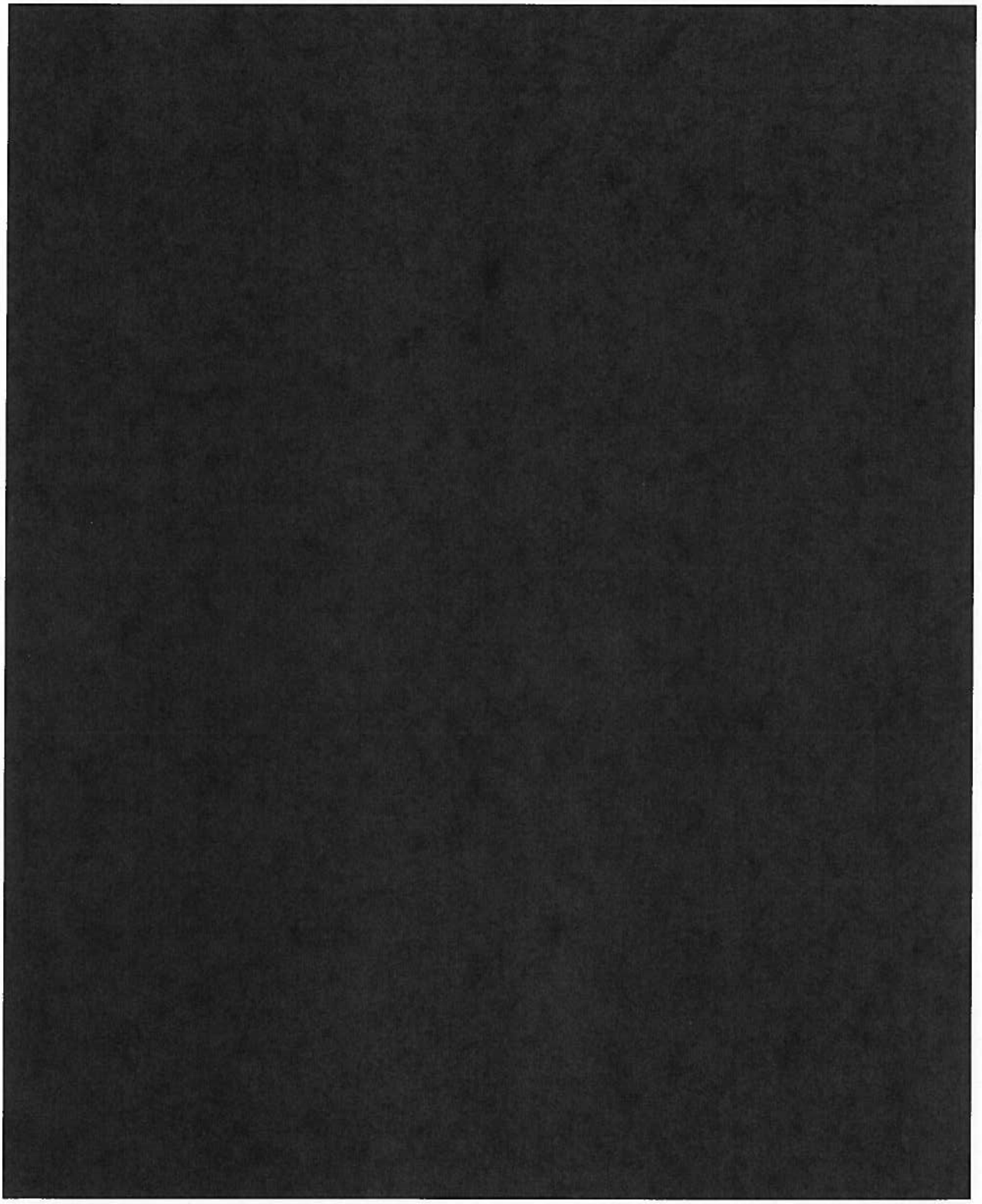




ST-09-0002 ~~TOP SECRET//STLW//COMINT//ORCON/NOFORN~~



~~TOP SECRET//STLW//COMINT//ORCON/NOFORN~~



[redacted]

(U//~~FOUO~~) Signature of President

~~(TS//STLW//SI//OC/NF)~~ The Authorizations were signed by the President, followed by a place and date of signature. All but one authorization was signed in Washington, D.C.

(U) Other Signatures

~~(TS//STLW//SI//OC/NF)~~ Under the phrase "approved for form and legality," the Attorney General signed all but one of the Authorizations. The other authorization and the two modifications were signed by the Counsel to the President.

[redacted]

APPENDIX C

(U) Timeline of Key Events

This page intentionally left blank.

(U) Timeline of Key Events

(U//~~FOUO~~) This timeline includes key events that occurred during NSA's implementation of the President's Surveillance Program (PSP). In addition to issuances of the Authorization, the timeline includes selected communications between NSA and Congress, the Foreign Intelligence Surveillance Court (FISC), [redacted] Because the timeline is limited to documented events and communications, it is not all-inclusive.

~~(TS//STLW//SI//OC/NF)~~

Date	Event
2001	
4-Oct-01	**1st Presidential Authorization signed**
4-Oct-01	General Hayden briefs White House (President, Vice President [VP], VP Counsel, VP Chief of Staff, White House Counsel)
[redacted]	[redacted]
25-Oct-01	NSA briefs Chair and Ranking Member of House Permanent Select Committee on Intelligence (HPSCI), Chair and Vice Chair of Senate Select Committee on Intelligence (SSCI)
2-Nov-01	**2nd Presidential Authorization signed**
[redacted]	[redacted]
14-Nov-01	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
30-Nov-01	**3rd Presidential Authorization signed**
4-Dec-01	NSA briefs Chair, Senate Defense Appropriations Subcommittee, and Ranking Member, Senate Defense Appropriations Subcommittee
5 Dec 01	NSA briefs FBI Director Mueller
[redacted]	[redacted]
2002	
9-Jan-02	**4th Presidential Authorization signed**
[redacted]	[redacted]
11-Jan-02	NSA briefs Department of Justice, Office of Intelligence Policy and Review (DoJ, OIPR), James Baker
31-Jan-02	NSA briefs FISC Presiding Judge Lamberth
[redacted]	[redacted]
5-Mar-02	NSA briefs Chair and Ranking Member, HPSCI, and Vice Chair, SSCI
14-Mar-02	**5th Presidential Authorization signed**
[redacted]	[redacted]

Date	Event
10-Apr-02	NSA briefs Chair SSCI
18-Apr-02	**6th Presidential Authorization signed** [redacted]
17-May-02	NSA briefs incumbent FISC Presiding Judge Kollar-Kotelly
22-May-02	**7th Presidential Authorization signed** [redacted]
12-Jun-02	NSA briefs Chair, HPSCI, and Ranking Member HPSCI
24-Jun-02	**8th Presidential Authorization signed** [redacted]
8-Jul-02	NSA briefs Chair and Ranking Member SSCI
30-Jul-02	**9th Presidential Authorization signed** [redacted]
12-Aug-02	NSA briefs FISC Presiding Judge Kollar-Kotelly at the White House
13-Aug-02	NSA Inspector General (IG) cleared for the PSP
10-Sep-02	**10th Presidential Authorization signed**
11-Sep-02	NSA GC, Deputy General Counsel (GC), Associate GC for Operations, and IG meet to discuss PSP oversight [redacted]
18-Sep-02	1st NSA Due Diligence Meeting
30-Sep-02	Chair HPSCI visits NSA for briefing [redacted]
15-Oct-02	**11th Presidential Authorization signed** [redacted]
18-Nov-02	**12th Presidential Authorization signed** [redacted]
16-Dec-02	NSA IG advises General Hayden to issue "Delegation of Authority Letters" to "units that administer the project"
2003	
8-Jan-03	**13th Presidential Authorization signed** [redacted]

Date	Event
[redacted]	[redacted]
13-Jan-03	FBI Director visits NSA for briefing
29-Jan-03	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
7-Feb-03	**14th Presidential Authorization signed**
[redacted]	[redacted]
4-Mar-03	General Hayden issues first Delegation of Authority letter to key Signals Intelligence (SIGINT) Directorate operational personnel
[redacted]	
17-Mar-03	**15th Presidential Authorization signed**
[redacted]	[redacted]
22-Apr-03	**16th Presidential Authorization signed**
[redacted]	[redacted]
11-Jun-03	**17th Presidential Authorization signed**
[redacted]	[redacted]
14-Jul-03	**18th Presidential Authorization signed**
[redacted]	[redacted]
17-Jul-03	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
[redacted]	[redacted]
10-Sep-03	**19th Presidential Authorization signed**
[redacted]	[redacted]

Date	Event
8-Oct-03	NSA-FBI-CIA conference at NSA to discuss PSP operations and customer needs
15-Oct-03	**20th Presidential Authorization signed**
[redacted]	[redacted]
1-Dec-03	NSA IG announces a review of NSA PSP operations
8-Dec-03	NSA IG asks VP Counsel for access to PSP legal opinions and is told that a request should come from General Hayden
9-Dec-03	**21st Presidential Authorization signed**
9-Dec-03	IG memo asks General Hayden to ask VP Counsel's permission for NSA IG and GC to obtain copies of, or view, PSP legal justification
[redacted]	[redacted]
2004	
6-Jan-04	NSA briefing to DoJ Mr. Philbin, Mr. Goldsmith for Mr. Goldsmith's orientation to the PSP and other NSA Signals Intelligence efforts against terrorism
8-Jan-04	NSA and FBI [redacted] meet to discuss the PSP and recent changes at NSA
14-Jan-04	**22nd Presidential Authorization signed**
[redacted]	[redacted]
9-Mar-04	General Hayden briefs Director of Central Intelligence (DCI) on value of the PSP
10-Mar-04	General Hayden briefs White House Counsel and Chief of Staff, Deputy DCI, Deputy AG, and FBI Director on value of the PSP
10-Mar-04	General Hayden briefs Speaker of the House, Senate Majority and Minority leaders, House Minority Leader, Chairman and Ranking Member, HPSCI, and Chair and Vice Chair, SSCI
10-Mar-04	General Hayden briefs Secretary of Defense, DoD Principal Deputy GC
11-Mar-04	**23rd Presidential Authorization signed**
11-Mar-04	NSA IG and Acting GC discuss new Authorization signed by President's Counsel rather than the AG
11-Mar-04	NSA briefs House Majority Leader
[redacted]	[redacted]
12-Mar-04	General Hayden briefs House Majority Leader
19-Mar-04	**Revision to 23rd Presidential Authorization signed**
[redacted]	General Hayden sends letter to Assistant AG, Office of Legal Counsel (OLC) [redacted]

Date	Event
	[redacted]
2-Apr-04	**2nd Revision to 23rd Presidential Authorization signed**
4-Apr-04	General Hayden briefs DoD Principal Deputy GC
5-May-04	**24th Presidential Authorization signed**
[redacted]	[redacted]
20-May-04	NSA briefs the Minority Leader of the Senate
[redacted]	[redacted]
23-Jun-04	**25th Presidential Authorization signed**
[redacted]	[redacted]
14-Jul-04	Initial PR/TT Order approved by FISC
9-Aug-04	**26th Presidential Authorization signed**
[redacted]	[redacted]
23-Aug-04	General Hayden briefs National Security Advisor and Homeland Security Advisor
[redacted]	
17-Sep-04	**27th Presidential Authorization signed**
[redacted]	[redacted]
23-Sep-04	Presidential "further direction" of 9 August 2004 expires
23-Sep-04	NSA briefs Chair, HPSCI
[redacted]	
17-Nov-04	**28th Presidential Authorization signed**
[redacted]	[redacted]
2005	
5-Jan-05	NSA briefs National Security Advisor and White House Counsel
[redacted]	[redacted]
11-Jan-05	**29th Presidential Authorization signed**

Date	Event
[redacted]	[redacted]
3-Feb-05	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
25-Feb-05	General Hayden briefs White House Counsel and Counsel to Deputy AG
1-Mar-05	**30th Presidential Authorization signed**
2-Mar-05	NSA briefs Senate Minority Leader
[redacted]	[redacted]
19-Apr-05	**31st Presidential Authorization signed**
[redacted]	[redacted]
22-Apr-05	General Hayden briefs Director of National Intelligence (DNI)
23-May-05	Two-level PSP clearance structure discontinued
1-Jun-05	Discussions to seek FISC orders to authorize content collection begin with DoJ OLC
14-Jun-05	**32nd Presidential Authorization signed**
[redacted]	[redacted]
26-Jul-05	**33rd Presidential Authorization signed**
[redacted]	[redacted]
3-Aug-05	Principal Deputy DNI Hayden briefs new NSA/CSS Director General Alexander on the PSP
10-Sep-05	**34th Presidential Authorization signed**
14-Sep-05	NSA briefs Chair and Ranking Member, HPSCI, Chair and Vice Chair, SSCI
[redacted]	[redacted]
26-Oct-05	**35th Presidential Authorization signed**
[redacted]	[redacted]
13-Dec-05	**36th Presidential Authorization signed**
16-Dec-05	New York Times says that President secretly authorized NSA eavesdropping on Americans
[redacted]	[redacted]
20-Dec-05	DoD IG receives letter, signed by 39 Congressmen, requesting a review of the PSP. DoD IG faxes the letter to the NSA IG on 10 Jan 06
21-Dec-05	NSA briefs DNI

Date	Event
2006	
3-Jan-06	NSA IG and DoD IG discuss letter from 39 Congressmen requesting DoD IG review of the PSP
9-Jan-06	NSA briefs nine FISC judges and three FISC legal advisors
11-Jan-06	NSA briefs Speaker of the House, Senate Majority Leader, Chair of HPSCI, Chair and Vice Chair, SSCI
20-Jan-06	NSA briefs Senate Minority Leader, House Minority Leader, Chair SSCI, and Ranking Member HPSCI
[redacted]	[redacted]
27-Jan-06	**37th Presidential Authorization signed**
31-Jan-06	NSA briefs FISC Judge Scullin
[redacted]	[redacted]
11-Feb-06	NSA briefs Chair SSCI
16-Feb-06	NSA briefs Speaker of the House and Chair, HPSCI
28-Feb-06	NSA briefs Chair and Ranking Member, House Appropriations Subcommittee on Defense
[redacted]	
3-Mar-06	NSA briefs Vice Chair, SSCI
9-Mar-06	NSA briefs Chair and Vice Chair, SSCI, and Members of SSCI Terrorist Surveillance Program (TSP) Subcommittee (Roberts, Rockefeller, Hatch, DeWine, Feinstein, Levin, Bond) with SSCI Minority and Majority Staff Directors, Senior Director for Legislative Affairs, National Security Counsel, VP, AG, White House Counsel, and VP Chief of Staff
10-Mar-06	NSA briefs Mr. Bond, Member, SSCI TSP Subcommittee
13-Mar-06	NSA briefs Chair, SSCI TSP Subcommittee, Members SSCI TSP Subcommittee (Roberts, Feinstein, and Hatch), SSCI Majority and Minority Staff Directors, and SSCI Counsel at NSA
14-Mar-06	NSA briefs Mr. DeWine, Member, SSCI TSP Subcommittee at NSA
21-Mar-06	**38th Presidential Authorization signed**
21-Mar-06	NSA briefs FISC Judge Bates
[redacted]	[redacted]
27-Mar-06	NSA briefs Mr. Levin, Member, SSCI TSP Subcommittee and Minority Staff Director at NSA
29-Mar-06	NSA briefs Chairman and Ranking Member HPSCI TSP Subcommittee, TSP Subcommittee Members (Hoekstra, Harman, McHugh, Rogers, Thornberry, Wilson, Davis, Holt, Cramer, Eshoo, and Boswell), Majority General Counsel, Staff Member, and Minority General Counsel

Date	Event
7-Apr-06	NSA briefs Chairman of the HPSCI TSP Subcommittee, HPSCI TSP Subcommittee Members (Hoekstra, McHugh, Rogers, Thornberry, Wilson, and Holt), Majority General Counsel, Staff Member, and Minority General Counsel at NSA
[redacted]	[redacted]
28-Apr-06	NSA briefs Ranking Member, HPSCI TSP Subcommittee, Members of HPSCI TSP Subcommittee (Harman, Wilson, and Eshoo), Majority General Counsel, Staff Member, and Minority General Counsel at NSA
[redacted]	
11-May-06	NSA briefs Chair and Ranking Member House Appropriations Committee Defense Subcommittee
16-May-06	**39th Presidential Authorization signed**
17-May-06	Chair SSCI, Members, SSCI (Roberts, Hagel, Mikulski, Snowe, DeWine, Bayh, Chambliss, Lott, Bond, Levin, Feingold, Feinstein, Wyden, Warner), SSCI Staff Member, SSCI Majority Staff Director, and SSCI Counsel
17-May-06	HPSCI Chair, HPSCI Members (Hoekstra, Harman, Wilson, Eshoo, Rogers, Thornberry, Holt, Boswell, Cramer, LaHood, Everett, Gallegly, Davis, Tiahrt, Reyes, Ruppersberger, and Tierney), Majority General Counsel, Staff Director, and Minority General Counsel
[redacted]	[redacted]
24-May-06	First Business Records Order approved by the FISC
5-Jun-06	NSA briefs Ms. Feingold, SSCI Member at NSA
7-Jun-06	NSA briefs Ranking Member, Senate Defense Appropriations Subcommittee, and SSCI Staff Director
7-Jun-06	NSA briefs President's Privacy and Civil Liberties Oversight Board
9-Jun-06	NSA briefs Chair, SSCI, SSCI Members (Mikulski, Wyden, and Hagel), SSCI Minority Staff Director, SSCI Counsel, and SSCI Staff Director
15-Jun-06	NSA briefs Chair, SSCI and SSCI Members (Roberts, Mikulski, Feingold, Bayh, Snowe, Hatch, Lott, and Bond), and Minority Staff Director
26-Jun-06	NSA briefs Chair, Senate Defense Appropriations Subcommittee, and House Minority Leader
30-Jun-06	NSA briefs Mr. Bayh, SSCI Member at NSA
6-Jul-06	**40th Presidential Authorization signed**
[redacted]	[redacted]
10-Jul-06	NSA briefs Ms. Snowe, SSCI Member and SSCI Counsel at NSA
18-Jul-06	NSA briefs Mr. Chambliss, SSCI Member at NSA
[redacted]	
6-Sep-06	**41st Presidential Authorization signed**
[redacted]	[redacted]

Date	Event
[redacted]	[redacted]
24-Oct-06	**42nd Presidential Authorization signed**
[redacted]	[redacted]
20-Nov-06	NSA briefs President's Privacy and Civil Liberties Oversight Board
8-Dec-06	**43rd and final Presidential Authorization signed**
[redacted]	[redacted]

2007

10-Jan-07	Content orders approved by the FISC
17-Jan-07	AG letter to Congress: Presidential program brought under the FISC
1-Feb-07	NSA briefs President's Privacy and Civil Liberties Oversight Board
1-Feb-07	Presidential Authorization expires

~~(TS//STLW//SI//OC/NF)~~

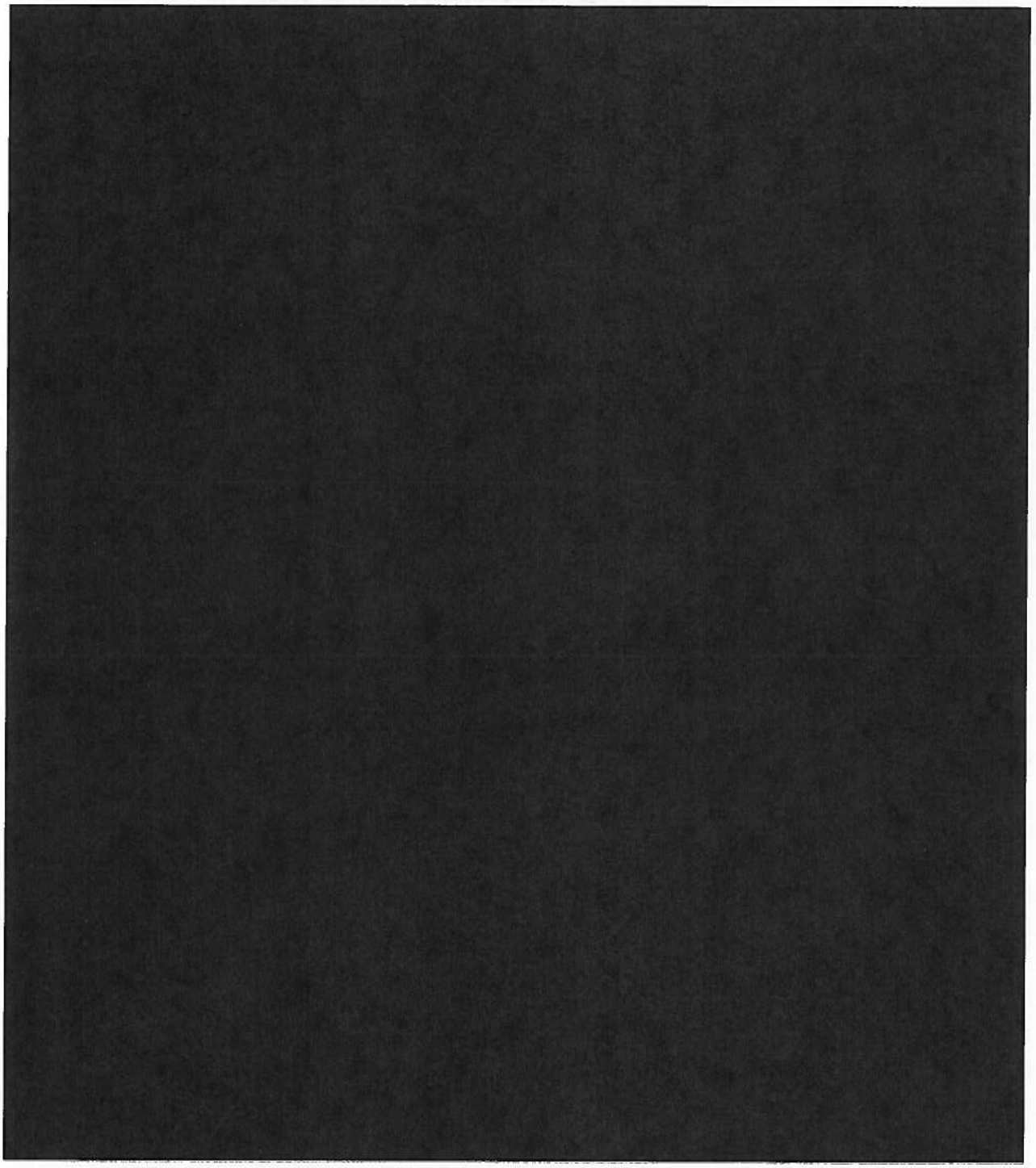
This page intentionally left blank.

APPENDIX D

(U) Cumulative Number of Clearances for the President's Surveillance Program

This page intentionally left blank.

(U) Cumulative Number of Clearances for the President's Surveillance Program[4]



This page intentionally left blank.

APPENDIX E

(U) NSA Office of the Inspector General Reports on the President's Surveillance Program and Related Activities

This page intentionally left blank.

(U) NSA Office of the Inspector General Reports on the President's Surveillance Program and Related Activities

~~(TS//SI//NF)~~ This appendix lists and describes OIG investigation and review reports of activity conducted under the PSP, also referred to as the STELLARWIND Program, and related activities such as the Pen Register Trap and Trace (PR/TT) Order and the Business Records Order. These reports are limited to activity conducted between 4 October 2001 and 17 January 2007.

(U) OIG Investigations

[redacted]

(U) Report of Investigation of Two Violations

~~(S//NF)~~ On [redacted] the OIG issued a report on what it believed to be the first two violations of Authorization, both of which were unintentional.

~~(TS//STLW//SI//OC/NF)~~ The first incident occurred on [redacted] An NSA analyst misguidedly used PSP authority to collect communications between [redacted] These communications were foreign within the meaning of the Authorization, but they were not terrorist related. [redacted]

~~(TS//STLW//SI//OC/NF)~~ The second incident occurred on [redacted] when NSA inappropriately performed contact chaining on [redacted] This query was requested by an FBI official during the investigation of [redacted]

~~(S//NF)~~ NSA OIG found that in neither incident had NSA personnel acted with intent to disregard their authority.

Both incidents occurred, at least in part, because early in the Program the terms of the Authorization were so closely held that few, if any, operational personnel working under the Authority were permitted to see the Authorization or its operative provisions. It was unreasonable to hold persons accountable for violating an order that they had not seen, when the order was too complex to be easily committed to memory. Accordingly, the OIG did not recommend disciplinary action, but did recommend that the NSA Director issue formal written delegations of authority to the Signals Intelligence Director and specified subordinates so that personnel working the Program would know the precise terms of the Authorization. Management concurred with the recommendations and made appropriate notifications.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008.

[redacted] ~~(TS//SI//NF)~~ ***Violations of Court Orders in*** [redacted]

Foreign Intelligence Surveillance Court

~~(TS//STLW//SI//OC/NF~~ On 14 July 2004 [redacted] The Order permitted NSA to collect Internet metadata under the pen register/trap-and-trace provisions of the FISA (§§ 1841-1846). The authority to collect Internet metadata under the Order [redacted] Material acquired under the Order continued to be protected in PSP channels.

~~(TS//STLW//SI//OC/NF)~~ On [redacted] NSA OIG issued a report on an investigation of a management breakdown that had resulted in unintentional filtering violations of the FISC Order. The Order permitted NSA to collect Internet metadata from communications involving [redacted] The violations occurred because NSA [redacted] However, no violations resulted from the collection of domestic communications. An NSA collection manager discovered the violations on [redacted]. The following day, the questionable collection was stopped and reported to the OIG and the OGC. With the exception of [redacted] the OIG

found no reason to believe that any violations resulted in the collection of U.S. person information. The OIG reserved judgment on [redacted] The OIG evaluation of responsibility for the incident led directly to the replacement of the Program Manager and to changes in Program management, leadership, and chain of command.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

[redacted]

(~~TS//SI//NF~~) Supplemental Report on Violations of Court Orders in [redacted]

~~(TS//STLW//SI//OC/NF)~~ A follow-up investigation of the questionable [redacted] revealed no additional violations. On [redacted], the NSA OIG issued a report detailing its examination of [redacted] that the OIG suspected might not have originated or terminated outside the United States. [redacted] All but [redacted] messages could have been associated with a foreign sender or recipient. [redacted] None of the [redacted] messages had been intentionally collected, none had been analyzed, and none had been reported outside NSA.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008.

(U) OIG Reviews

14 May 2004 ***(U) Need for Documentation and Development of Key Processes (ST-04-0024)***

~~(TS//SI//NF)~~ This OIG report concluded that a continuing deficiency in clear, written procedures governing the collection, processing, and dissemination of PSP material created undue risk of unintentional violations of the Authorization. The report noted that Program officials had

made progress in addressing some of these deficiencies, but found that processes had not been fully documented in the form of management directives, administrative policies, or operating manuals. The NSA OIG recommended that Program officials formally adopt rigorous, written operating procedures for the following key processes:

- Approvals for content collection by the appropriate named officials
- Reporting of violations of the Authority, similar to procedures for documenting violations of Legal Compliance and Minimization Procedures[5]
- Evaluation of dual FISA and PSP content collection
- Systematic identification and evaluation of telephone numbers and Internet identifiers for detasking.[6]

(U//~~FOUO~~) Corrective action was taken in response to the four recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 06 and HPSCI on 2 January 2008.

13 Sep 2004 ***~~(S//NF)~~ Need for Increased Attention to Security-Related Aspects of the STELLARWIND Program (ST-04-0025)***

(U//~~FOUO~~) This OIG report disclosed weaknesses in Program security. The Program was particularly vulnerable to exposure because it involved numerous organizations inside and outside NSA.

(U//~~FOUO~~) While the Program Manager placed a strong emphasis on personnel security, he did not take a proactive and strategic approach to physical and operational security. In particular, better use of the Program Security Officer would have helped to improve special security practices for handling Program material and strengthen operations security (OPSEC).

(U//~~FOUO~~) The Program Manager and the Associate Director for Security and Counterintelligence concurred with the findings and implemented corrective measures. In particular,

---

[5](U) U.S. Signals Intelligence Directive 18 or "USSID SP0018" (as of 27 July 2003).
[6](~~TS//SI//NF~~) [redacted]

the Staff Security Officer was freed from other responsibilities and took a more active and effective role in Program security. Management did not conduct a formal OPSEC survey as recommended; however, steps taken by management to implement OPSEC practices met the intent of the original recommendation.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008.

21 Nov 2005 ***~~(TS//SI//NF)~~ Review of the Tasking Process for STELLARWIND U.S. Content Collection (ST-04-0026)***

~~(TS//STLW//SI//OC/NF)~~ This report identified material weaknesses in the tasking and detasking process under the PSP. The process to task and detask telephone numbers for content collection under the Program was inherently fragile because it was based on e-mail exchanges and was not automated or monitored.

~~(TS//STLW//SI//OC/NF)~~ The OIG examined [redacted] telephone numbers and Internet identifiers approved for content collection on the date in November 2004 when the audit began and identified the following types of errors:

- [redacted] involved under-collection; identifiers were not put on collection quickly enough or were not put on collection until the OIG discovered the errors.
- [redacted] involved unauthorized collection caused by a typographical error.
- [redacted] involved over-collection; they were not removed from collection quickly enough.
- [redacted] record-keeping errors in the Program's tracking database

~~(TS//STLW//SI//OC/NF)~~ In the [redacted] of unauthorized collection caused by a typographical error, NSA personnel did not review the collected information before destroying it, nor did NSA issue any report based on, or otherwise disseminate, any information from the [redacted] of untimely detasking. However, without a robust and reliable collection and tracking process, NSA increased its risk of unintentionally violating the Authorization. NSA also increased the risk of missing

valuable foreign intelligence by failing to task telephone numbers and Internet identifiers in a timely manner.

(U//~~FOUO~~) NSA OIG recommended that all errors be swiftly resolved, that specific procedures be adopted to prevent recurrences, and that identifiers tasked for collection be promptly reconciled with identifiers approved for tasking, and repeated every 90 days. Management implemented the recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

31 May 2006 ~~(TS//SI//NF)~~ ***Review of Compliance with Authorization Requirements for STELLARWIND U.S. Content Collection (ST-04-0027)***

~~(TS//STLW//SI//OC/NF)~~ This report determined that, based on a statistical sample, Program officials were adhering to the terms of the Authorization and the Director's delegation thereunder; that tasking was appropriately approved and duly recorded under the Authorization; and that tasking was justified as linked to al-Qa'ida or affiliates of al-Qa'ida. The report recommended improvements in record-keeping practices.

~~(S//NF)~~ Due to a lack of sufficient and reliable data, the NSA OIG could not reach a conclusion on the tasking approval process for two PSP-related collection programs. The OIG recommended that management responsible for the affected programs, design and implement a tasking and tracking process to allow managers to audit, assess timeliness, and validate the sequencing of tasking activities. Management agreed to install automated tracking of tasking and detasking.

~~(TS//SI//NF)~~ Although the collection architecture was designed to produce one-end-foreign communications, inadvertent collection of domestic communications occurred and was addressed. The OIG recommended changes in management reporting to improve the tracking and resolution of inadvertent collection issues.

(U//~~FOUO~~) Corrective action has been completed for one of the two recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 31 May 2006 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

11 Jul 2006 ~~(TS//SI//NF)~~ ***Supplemental Report to Review of Compliance with Authorization Requirements for STELLARWIND U.S. Content Collection (ST-04-0027.01)***

~~(TS//STLW//SI//OC/NF)~~ After issuing the original report, the NSA OIG conducted further research to determine whether Program officials were approving content tasking requests based solely on metadata analysis. Using the statistical sample in the original audit, the OIG found no instances of metadata analysis as the sole justification for content tasking. In all cases tested, there was corroborating evidence to support the tasking decision.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008.

5 Sep 2006 ~~(TS//SI//NF)~~ ***Report on the Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance Court Order: Telephony Business Records (ST-06-0018)***

~~(TS//STLW//SI//OC/NF)~~ On 24 May 2006, the telephony metadata portion of the PSP was transferred to FISC Order BR-06-05, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from* [Telecommunications Providers] *Relating to* [redacted] The Order authorized NSA to collect and retain telephony metadata to protect against international terrorism and to process and disseminate this data regarding [redacted]

~~(TS//SI//NF)~~ On 10 July 2006, in a memorandum with the subject *FISA Court Order: Telephony Business Records (ST-06-0018)*, the NSA OIG issued "a report to the Director of NSA 45 days after the initiation of the activity [permitted by the Order] assessing the adequacy of the management controls for the processing and dissemination of U.S. person information." This report was issued with the Office of the General Counsel's concurrence as mandated by the Order.

~~(TS//SI//NF)~~ The "*Report on the Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance*

Court Order: Telephony Business Records (ST-06-0018)," 5 September 2006, provided the details of the findings of the 10 July memorandum and made formal recommendations to management.

~~(TS//SI//NF)~~ Management controls governing the processing, dissemination, data security, and oversight of telephony metadata and U.S. person information obtained under the Order were adequate and in several aspects exceeded the terms of the Order. However, due to the risk associated with the collection and processing of telephony metadata involving U.S. person information, the NSA OIG recommended three additional controls regarding collection procedures, reconciliation of audit logs, and segregation of duties.

~~(TS//SI//NF)~~ Collection Procedures

~~(TS//SI//NF)~~ During an OIG review of collection procedures, Program management discovered that NSA was obtaining [redacted] data that might not have been in keeping with the Order: [redacted] OGC advised that [redacted] data should have been suppressed from the incoming data flow. Immediately, management blocked the data from analysts' view. Further, working with the providers, Program management completed suppression of the suspect data on 11 October 2006 and agreed to implement additional procedures to prevent the collection of unauthorized data.

~~(TS//SI//NF)~~ Reconciliation of Audit Logs

~~(TS//SI//NF)~~ Management controls were not in place to verify that telephone numbers approved for querying were the only numbers queried. Although audit logs documented the queries of the archived metadata, the logs were not in a usable format, and Program management did not routinely use them to audit telephone numbers queried. Management concurred with the recommendation to conduct periodic reconciliations; however, action was contingent on the approval of a Program management request for two additional computer Programmers.

[redacted]

~~(C//NF)~~ Lack of Segregation of Duties

~~(C//NF)~~ The seven individuals with the authority to approve queries also had the ability to conduct queries under the Order. Standard internal control practices require that key duties and responsibilities be divided among different people to reduce the risk of error and fraud. Although Program management concurred with the finding, it could not implement the recommendation due to staffing and operational needs. As an alternative, Program management agreed to develop a process to monitor independently the queries of the seven individuals. This action plan was contingent on the development of usable audit logs recommended above.

(U//~~FOUO~~) Corrective action has been completed for one of the three recommendations.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008.

20 Dec 2006 ***~~(S//NF)~~ Summary of OIG Oversight 2001-2006 STELLARWIND Program Activities (ST-07-0011)***

~~(S//NF)~~ On 20 December 2006, the OIG issued a report summarizing OIG's oversight of the STELLARWIND Program after five years of implementation.

(U//~~FOUO~~) This report was sent to SSCI on 13 February 2007 and HPSCI on 2 January 2008 and was redacted at the request of the White House.

[redacted] ***~~(TS//SI//NF)~~ Assessment of Management Controls to Implement the FISC Order Authorizing NSA to Collect Information Using Pen Register and Trap and Trace Devices (ST-06-0020)***

~~(TS//SI//NF)~~ On [redacted] the OIG reported that the management controls governing the collection, dissemination, and data security of electronic communications metadata and U.S. person information obtained under the FISC Order authorizing NSA to collect Internet metadata using PR/TT devices were adequate and in several aspects exceeded the terms of the Order. Due to the risk associated with the processing of electronic communications metadata involving U.S. person information, additional controls were needed for processing and monitoring queries made against PR/TT data, documenting

oversight activities, and providing annual refresher training on the terms of the Order.

(U//~~FOUO~~) Corrective action has been completed for two of the six recommendations.

(U//~~FOUO~~) This report was sent to SSCI on [redacted] and HPSCI on [redacted]

5 Jul 2007 ***~~(TS//SI//NF)~~ Domestic Selector Tasking Justification Review (ST-07-0017)***

(U//~~FOUO~~) The OIG conducted this review to determine whether tasking justification statements were supported with intelligence information consistent with sources cited in the justifications. The OIG identified some justifications containing errors, but there was no pattern of errors or exaggeration of facts or intentional misstatements.

(U//~~FOUO~~) This report was sent to SSCI on 28 January 2008 and HPSCI on 28 January 2008.

30 June 2008 ***~~(TS//SI//NF)~~ Advisory Report on the Adequacy of STELLARWIND Decompartmentation Plans (ST-08-0018)***

~~(TS//SI//NF)~~ At the request of the SID Program Manager for CT Special Projects, the OIG assessed the adequacy of NSA's plans to remove data from the STELLARWIND compartment, as authorized by the Director of National Intelligence. On 30 June 2008, the OIG reported that NSA management had a solid foundation of planning for decompartmentation. In particular, the content, communication, and assignment of supporting plans were adequate to provide reasonable assurance of successfully removing data from the STELLARWIND compartment, while complying with laws and authorities. Management was also diligent in assessing the scope and complexity of this undertaking. Although the OIG made no formal recommendations, it suggested improvements to develop more detailed plans, set firm milestones, and establish a feedback system to ensure that plans were successfully implemented.

(U//~~FOUO~~) This report was not sent to SSCI or HPSCI.

APPENDIX F

(U) Presidential Notifications

This page intentionally left blank.

(U) Presidential Notifications

~~(TS//STLW//SI//OC/NF)~~ Executive Orders 12333 and 12863 require intelligence agencies to report to the President, through the President's Intelligence Oversight Board, activities they have reason to believe may be unlawful or contrary to executive order or presidential directive. Knowing that Board members were not cleared, however, the NSA Director or Deputy Director reported the following violations of the Presidential Authorization and related authorities to the President through his Counsel, rather than through the Board. Each notification was approved if not actually drafted by OIG. Some of the notifications were not the subject of the OIG reviews or investigations discussed in Appendix E.

(U) Date	(U) Summary of Notification
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes violations regarding (1) the [redacted] and (2) [redacted]
[redacted]	[redacted]
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes a delay of about 90 days in detasking a telephone number [redacted]
[redacted]	~~(TS//SI//NF)~~ Describes the investigation mentioned above regarding metadata collection violations that occurred under FISA Court Order *In Re* [redacted] FISA Court [redacted] The complete OIG report was issued [redacted]
[redacted]	~~(TS//SI//NF)~~ Describes [redacted] instances in which cleared NSA analysts mistakenly accessed data [redacted] In one instance, a report based on such data went out, but it was not cancelled because the same information was available elsewhere. In the other [redacted] instances, no reports were issued. [redacted]

(U) Date	(U) Summary of Notification
	[redacted]
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes one instance of inadvertent collection of a call with both ends in the U.S. – a fact that could not have been known until it was listened to because [redacted] showed the call as having a foreign origin. [redacted]
[redacted]	~~(TS//SI//NF)~~ Describes three incidents: The first involved a one-digit typo resulting in one incorrectly tasked number. The second involved a number improperly tasked for metadata analysis. The operator discovered it almost immediately and promptly removed it from tasking. The third involved [redacted] numbers that were not detasked in a timely fashion.
2 Aug 2005 [redacted]	~~(TS//SI//NF)~~ Describes the evolving [redacted] a practice that may have resulted in over-collection. The notification refers to NSA's work in developing more rigorous [redacted]
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes an incident in which bulk telephony metadata was actively collected in spite [redacted] At that time NSA limited collection of bulk telephone records to [redacted] as permitted by statute. The collection resulted when [redacted] The error was not discovered for 18 months. ~~(TS//STLW//SI//OC/NF)~~ Although most of the metadata improperly collected was also properly acquired [redacted] pursuant to statute, the dataflow was terminated immediately upon discovery. Also, because the improperly collected metadata had been forwarded to non-STELLARWIND databases, the Agency removed non-compliant metadata from all affected databases, including those in which STELLARWIND data is normally stored.

(U) Date	(U) Summary of Notification
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case, [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes an incident in which an [redacted] This resulted [redacted] of non-target data. The error was discovered within hours, when personnel responsible for monitoring [redacted] The error was corrected, and all inadvertently collected records were deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case, [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes [redacted] instances in which authorized targeting of properly tasked [redacted] telephone numbers resulted in inadvertent collection of U.S.-to-U.S. calls. In each case, [redacted] No reporting was generated, and collection was deleted.
[redacted]	~~(TS//STLW//SI//OC/NF)~~ Describes an instance where a [redacted] Although no reports were generated, and there was no evidence that U.S.-to-U.S. communications were collected, we could not certify that the files were all one-end foreign without reviewing [redacted] The [redacted] files were deleted, and procedures used by [redacted] were being reviewed. ~~(TS//STLW//SI//OC/NF)~~ A second incident was reported in which a typographical error resulted in contact chaining on a U.S. telephone number with no [redacted] affiliation. The telephone number was rechecked, and the error was corrected.

This page intentionally left blank.

APPENDIX G

(U) United States Signals Intelligence Directive SP0018, Legal Compliance and Minimization Procedures

APPROVED FOR PUBLIC RELEASE

This page intentionally left blank.

AUTHORIZED REPRODUCTION NUMBER 00R0043

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

Fort George G. Meade, Maryland

UNITED STATES

SIGNALS INTELLIGENCE

DIRECTIVE

18

27 July 1993

INCLUDES CHANGES 1 and 2

See Letter of Promulgation for instructions on reproduction or release of this document.

~~OPC: D2~~
~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

This page intentionally left blank.

~~SECRET~~

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
Fort George G. Meade, Maryland

27 July 1993

UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE

(USSID)

18

LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES ~~(FOUO)~~

LETTER OF PROMULGATION

(U) This USSID prescribes policies and procedures and assigns responsibilities to ensure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights of U.S. persons.

(U) This USSID has been completely rewritten to make it shorter and easier to understand. It constitutes a summary of the laws and regulations directly affecting USSS operations. All USSS personnel who collect, process, retain, or disseminate information to, from, or about U.S. persons or persons in the United States must be familiar with its contents.

~~(FOUO)~~ This USSID supersedes USSID 18, and USSID 18, Annex A (distributed separately to selected recipients), both of which are dated 20 October 1980, and must now be destroyed. Notify DIRNSA/CHCSS (USSID Manager) if this edition of USSID 18 is destroyed because of an emergency action; otherwise, request approval from DIRNSA/CHCSS before destroying this USSID.

~~(FOUO)~~ Release or exposure of this document to contractors and consultants without approval from the USSID Manager is prohibited. Instructions applicable to release or exposure of USSID to contractors and consultants may be found in USSID 19.

~~(FOUO)~~ Questions and comments concerning this USSID should be addressed to the Office of the General Counsel, NSA/CSS, NSTS 963-3121 or [redacted]

J.M.McCONNELL
Vice Admiral, U.S. Navy
Director

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

APPROVED FOR PUBLIC RELEASE

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

This page intentionally left blank.

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

USSID 18
27 July 1993

CHANGE REGISTER

No	Date	CHANGE Authority (Msg Cite/DTG, Hard Copy (HC))	ENTERED Date	By
1	28OCT97	HARDCOPY CHANGE	29OCT97	RS
2	11Dec98	P0211-0307-98, 111800Z Dec 98	11Dec98	WF
2	11Dec98	P0211-0309-98, 111840Z Dec 98 (correction to above)	11Dec98	WF

APPROVED FOR PUBLIC RELEASE

This page intentionally left blank.

TABLE OF CONTENTS

SECTION 1 – PREFACE 1

SECTION 2 – REFERENCES 1

SECTION 3 – POLICY 2

SECTION 4 – COLLECTION 2

4.1. Communications to, from or About U.S. Persons and [redacted] 2

a. Foreign Intelligence Surveillance Court Approval 2

b. Attorney General Approval 2

c. DIRNSA/CHCSS Approval 2

d. Emergency Situations 3

e. Annual Reports 4

4.2. [redacted] 4

4.3. Incidental Acquisition of U.S. Person Information 4

4.4. Nonresident Alien Targets Entering the United States 5

4.5. U.S. Person Targets Entering the United States 5

4.6. Requests to Target U.S. Persons 5

4.7. Direction Finding 5

4.8. Distress Signals 5

4.9. COMSEC Monitoring and Security Testing of Automated Information Systems 6

SECTION 5 – PROCESSING 6

5.1. Use of Selection Terms During Processing 6

5.2. Annual Review by DDO 6

5.3. Forwarding of Intercepted Material 6

5.4. Nonforeign Communications 7

a. Communications between Persons in the United States 7

b. Communications between U.S. Persons 7

c. Communications Involving an Officer or Employee of the U.S. Government 7

d. Exceptions 7

5.5. Radio Communications with a Terminal in the United States 7

SECTION 6 – RETENTION 8

6.1. Retention of Communications to, from, or About U.S. Persons 8

a. Unenciphered Communications; and Communications Necessary to Maintain Technical Data Bases for Cryptanalytic or Traffic Analytic Purposes 8

b. Communications Which Could be Disseminated Under Section 7 8

6.2. Access 8

SECTION 7 – DISSEMINATION 8

7.1. Focus of SIGINT Reports 8

7.2. Dissemination of U.S. Person Identities 9

a. Consent 9

b. Publicly Available Information 9

c. Information Necessary to Understand or Access 9

7.3. Approval Authorities 10

a. DIRNSA/CHCSS 10

b. Field Units 10

c. DDO and Designees 10

7.4. Privileged Communications and Criminal Activity 10

7.5. Improper Dissemination 10

SECTION 8 – RESPONSIBILITIES 11

8.1. Inspector General 11

8.2. General Counsel 11

8.3. Deputy Director for Operations 12

8.4. All Elements of the USSS 12

SECTION 9 – DEFINITIONS 12

ANNEX A – PROCEDURES IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (U) A/1

APPENDIX 1 – STANDARIZED MINIMIZATION PROCEDURES FOR NSA ELECTRONIC SURVEILLANCES A–1/1

ANNEX B – OPERATIONAL ASSISTANCE TO THE FEDERAL BUREAU OF INVESTIGATION (U) B/1

ANNEX C – SIGNALS INTELLIGENCE SUPPORT TO U.S. AND ALLIED MILITARY EXERCISE COMMAND AUTHORITIES (U) C/1

ANNEX D – TESTING OF ELECTRONIC EQUIPMENT (U) D/1

ANNEX E – SEARCH AND DEVELOPMENT OPERATIONS (U) E/1

ANNEX F – ILLICIT COMMUNICATIONS ~~(C)~~ F/1

ANNEX G – TRAINING OF PERSONNEL IN THE OPERATION AND USE OF SIGINT COLLECTION AND OTHER SURVEILLANCE EQUIPMENT (U) G/1

ANNEX H – CONSENT FORMS (U) H/1

ANNEX I – FORM FOR CERTIFICATION OF OPENLY-ACKNOWLEDGED ENTITIES ~~(S-CCO)~~ I/1

ANNEX J – PROCEDURES FOR MONITORING RADIO COMMUNICATIONS OF SUSPECTED INTERNATIONAL NARCOTICS TRAFFICKERS ~~(S-CCO)~~ (Issued separately to selected recipients) J/1

ANNEX K – [redacted] K/1

APPROVED FOR PUBLIC RELEASE

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

This page intentionally left blank.

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~SECRET~~

27 July 1993

USSID 18

LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES (U)

SECTION 1 – PREFACE

1.1. (U) The Fourth Amendment to the United States Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government. The Supreme Court has ruled that the interception of electronic communications is a search and seizure within the meaning of the Fourth Amendment. It is therefore mandatory that signals intelligence (SIGINT) operations be conducted pursuant to procedures which meet the reasonableness requirements of the Fourth Amendment.

1.2. (U) In determining whether United States SIGINT System (USSS) operations are "reasonable," it is necessary to balance the U.S. Government's need for foreign intelligence information and the privacy interests of persons protected by the Fourth Amendment. Striking that balance has consumed much time and effort by all branches of the United States Government. The results of that effort are reflected in the references listed in Section 2 below. Together, these references require the minimization of U.S. person information collected, processed, retained or disseminated by the USSS. The purpose of this document is to implement these minimization requirements.

1.3. (U) Several themes run throughout this USSID. The most important is that intelligence operations and the protection of constitutional rights are not incompatible. It is not necessary to deny legitimate foreign intelligence collection or suppress legitimate foreign intelligence information to protect the Fourth Amendment rights of U.S. persons.

1.4. (U) Finally, these minimization procedures implement the constitutional principle of "reasonableness" by giving different categories of individuals and entities different levels of protection. These levels range from the stringent protection accorded U.S. citizens and permanent resident aliens in the United States to provisions relating to foreign diplomats in the U.S. These differences reflect yet another main theme of these procedures, that is, that the focus of all foreign intelligence operations is on foreign entities and persons.

SECTION 2 – REFERENCES

2.1. (U) References

a. 50 U.S.C. 1801, et seq., Foreign Intelligence Surveillance Act (FISA) of 1978, Public Law No. 95-511.

b. Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981.

c. DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," dated 25 April 1988.

d. NSA/CSS Directive No. 10-30, "Procedures Governing Activities of NSA/CSS that Affect U.S. Persons," dated 20 September 1990.

SECTION 3 – POLICY

3.1. (U) The policy of the USSS is to TARGET or COLLECT only FOREIGN COMMUNICATIONS. The USSS will not intentionally COLLECT communications to, from or about U.S. PERSONS or persons or entities in the U.S. except as set forth in this USSID. If the USSS inadvertently COLLECTS such communications, it will process, retain and disseminate them only in accordance with this USSID.

SECTION 4 – COLLECTION

4.1. ~~(S-CCO)~~ Communications which are known to be to, from or about a U.S. PERSON [redacted] will not be intentionally intercepted, or selected through the use of a SELECTION TERM, except in the following instances:

a. With the approval of the United States Foreign Intelligence Surveillance Court under the conditions outlined in Annex A of this USSID.

b. With the approval of the Attorney General of the United States, if:

(1) The COLLECTION is directed against the following:

(a) Communications to or from U.S. PERSONS outside the UNITED STATES, or

(b) International communications to, from, [redacted], or

(c) Communications which are not to or from but merely about U.S. PERSONS (wherever located).

(2) The person is an AGENT OF A FOREIGN POWER, and

(3) The purpose of the COLLECTION is to acquire significant FOREIGN INTELLIGENCE information.

c. With the approval of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), so long as the COLLECTION need not be approved by the Foreign Intelligence Surveillance Court or the Attorney General, and

(1) The person has CONSENTED to the COLLECTION by executing one of the CONSENT forms contained in Annex H, or

* Capitalized words in Sections 3 through 9 are defined terms in Section 9.

(2) The person is reasonably believed to be held captive by a FOREIGN POWER or group engaged in INTERNATIONAL TERRORISM, or

(3) The TARGETED [redacted] and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex I, or

(4) The COLLECTION is directed against [redacted] between a U.S. PERSON in the UNITED STATES and a foreign entity outside the UNITED STATES, the TARGET is the foreign entity, and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex K, or

(5) Technical devices (e.g. [redacted]) are employed to limit acquisition by the USSS to communications to or from the TARGET or to specific forms of communications used by the TARGET (e.g., [redacted]) and the COLLECTION is directed against [redacted] voice and facsimile communications with one COMMUNICANT in the UNITED STATES, and the TARGET of the COLLECTION is [redacted]:

(a) A non-U.S. PERSON located outside the UNITED STATES [redacted]

(b) [redacted]

(6) Copies of approvals granted by the DIRNSA/CHCSS under these provisions will be retained in the Office of General Counsel for review by the Attorney General.

d. Emergency Situations.

(1) In emergency situations, DIRNSA/CHCSS may authorize the COLLECTION of information to, from, or about a U.S. PERSON who is outside the UNITED STATES when securing the prior approval of the Attorney General is not practical because:

(a) The time required to obtain such approval would result in the loss of significant FOREIGN INTELLIGENCE and would cause substantial harm to the national security.

(b) A person's life or physical safety is reasonably believed to be in immediate danger.

(c) The physical security of a defense installation or government property is reasonably believed to be in immediate danger.

(2) In those cases where the DIRNSA/CHCSS authorizes emergency COLLECTION, except for actions taken under paragraph d.(1)(b) above, DIRNSA/CHCSS shall find that there is probable cause that the TARGET meets one of the following criteria:

(a) A person who, for or on behalf of a FOREIGN POWER, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process),

sabotage, or INTERNATIONAL TERRORIST activities, or activities in preparation for INTERNATIONAL TERRORIST activities; or who conspires with, or knowingly aids and abets a person engaging in such activities.

(b) A person who is an officer or employee of a FOREIGN POWER.

(c) A person unlawfully acting for, or pursuant to the direction of, a FOREIGN POWER. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the FOREIGN POWER.

(d) A CORPORATION or other entity that is owned or controlled directly or indirectly by a FOREIGN POWER.

(e) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

(3) In all cases where emergency collection is authorized, the following steps shall be taken:

(a) The General Counsel will be notified immediately that the COLLECTION has started.

(b) The General Counsel will initiate immediate efforts to obtain Attorney General approval to continue the collection. If Attorney General approval is not obtained within seventy two hours, the COLLECTION will be terminated. If the Attorney General approves the COLLECTION, it may continue for the period specified in the approval.

e. Annual reports to the Attorney General are required for COLLECTION conducted under paragraphs 4.1.c.(3) and (4). Responsible analytic offices will provide such reports through the Deputy Director for Operations (DDO) and the General Counsel to the DIRNSA/CHCSS for transmittal to the Attorney General by 31 January of each year.

4.2. ~~(S-CCO)~~ [redacted]

a. [redacted]

b. [redacted]

4.3. (U) Incidental Acquisition of U.S. PERSON Information. Information to, from or about U.S. PERSONS acquired incidentally as a result of COLLECTION directed against appropriate FOREIGN INTELLIGENCE TARGETS may be retained and processed in accordance with Section 5 and Section 3 of this USSID.

4.4. ~~(S-CCO)~~ Nonresident Alien TARGETS Entering the UNITED STATES.

a. If the communications of a nonresident alien located abroad are being TARGETED and the USSS learns that the individual has entered the UNITED STATES, COLLECTION may continue for a period of 72 hours provided that the DIRNSA/CHCSS is advised immediately and:

(1) Immediate efforts are initiated to obtain Attorney General approval, or

(2) A determination is made within the 72 hour period that the [redacted]

b. If Attorney General approval is obtained, the COLLECTION may continue for the length of time specified in the approval.

c. If it is determined that [redacted] COLLECTION may continue at the discretion of the operational element.

d. If [redacted] or if Attorney General approval is not obtained within 72 hours, COLLECTION must be terminated [redacted] Attorney General approval is obtained, or the individual leaves the UNITED STATES.

4.5. ~~(C-CCO)~~ U.S. PERSON TARGETS Entering the UNITED STATES.

a. If communications to, from or about a U.S. PERSON located outside the UNITED STATES are being COLLECTED under Attorney General approval described in Section 4.1.b. above, the COLLECTION must stop when the USSS learns that the individual has entered the UNITED STATES.

b. While the individual is in the UNITED STATES, COLLECTION may be resumed only with the approval of the United States Foreign Intelligence Surveillance Court as described in Annex A.

4.6. ~~(S-CCO)~~ Requests to TARGET U.S. PERSONS. All proposals for COLLECTION against U.S. PERSONS, [redacted], must be submitted through the DDO and the General Counsel to the DIRNSA/CHCSS for review.

4.7. ~~(C-CCO)~~ Direction Finding. Use of direction finding solely to determine the location of a transmitter located outside of the UNITED STATES does not constitute ELECTRONIC SURVEILLANCE or COLLECTION even if directed at transmitters believed to be used by U.S. PERSONS. Unless COLLECTION of the communications is otherwise authorized under these procedures, the contents of communications to which a U.S. PERSON is a party monitored in the course of direction finding may only be used to identify the transmitter.

4.8. (U) Distress Signals. Distress signals may be intentionally collected, processed, retained, and disseminated without regard to the restrictions contained in this USSID.

4.9. (U) COMSEC Monitoring and Security Testing of Automated Information Systems. Monitoring for communications security purposes must be conducted with the consent of the person being monitored and in accordance with the procedures established in National Telecommunications and Information Systems Security Directive 600, Communications Security (COMSEC) Monitoring, dated 10 April 1990. Monitoring for

communications security purposes is not governed by this USSID. Intrusive security testing to assess security vulnerabilities in automated information systems likewise is not governed by this USSID.

SECTION 5 – PROCESSING

5.1. ~~(S-CCO)~~ Use of Selection Terms During Processing.
When a SELECTION TERM is intended to INTERCEPT a communication on the basis of the content of the communication, or because a communication is enciphered, rather than on the basis of the identity of the COMMUNICANT or the fact that the communication mentions a particular individual, the following rules apply:

a. No SELECTION TERM that is reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON (wherever located) [redacted] may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained by use of such SELECTION TERM.

b. No SELECTION TERM that has resulted in the INTERCEPTION of a significant number of communications to or from such persons or entities may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained.

c. SELECTION TERMS that have resulted or are reasonably likely to result in the INTERCEPTION of communications to or from such persons or entities shall be designed to defeat, to the greatest extent practicable under the circumstances, the INTERCEPTION of those communications which do not contain FOREIGN INTELLIGENCE.

5.2. ~~(S-CCO)~~ Annual Review by DDO.

a. All SELECTION TERMS that are reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON or terms that have resulted in the INTERCEPTION of a significant number of such communications shall be reviewed annually by the DDO or a designee.

b. The purpose of the review shall be to determine whether there is reason to believe that FOREIGN INTELLIGENCE will be obtained, or will continue to be obtained, by the use of these SELECTION TERMS.

c. A copy of the results of the review will be provided to the Inspector General and the General Counsel.

5.3. ~~(C-CCO)~~ Forwarding of Intercepted Material. FOREIGN COMMUNICATIONS collected by the USSS may be forwarded as intercepted to NSA, intermediate processing facilities, and collaborating centers.

5.4. ~~(S-CCO)~~ Nonforeign Communications.

a. Communications between persons in the UNITED STATES. Private radio communications solely between persons in the UNITED STATES inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be promptly destroyed unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

b. Communications between U.S. PERSONS. Communications solely between U.S. PERSONS will be treated as follows:

(1) Communications solely between U.S. PERSONS inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be destroyed upon recognition, if technically possible, except as provided in paragraph 5.4.d. below.

(2) Notwithstanding the preceding provision, cryptologic data (e.g., signal and encipherment information) and technical communications data (e.g., circuit usage) may be extracted and retained from those communications if necessary to:

(a) Establish or maintain intercept, or

(b) Minimize unwanted intercept, or

(c) Support cryptologic operations related to FOREIGN COMMUNICATIONS.

c. Communications Involving an Officer or Employee of the U.S. Government. Communications to or from any officer or employee of the U.S. Government, or any state or local government, will not be intentionally intercepted. Inadvertent INTERCEPTIONS of such communications (including those between foreign TARGETS and U.S. officials) will be treated as indicated in paragraphs 5.4.a. and b., above.

d. Exceptions: Notwithstanding the provisions of paragraphs 5.4.b. and c., the DIRNSA/CHCSS may waive the destruction requirement for international communications containing, inter alia, the following types of information:

(1) Significant FOREIGN INTELLIGENCE, or

(2) Evidence of a crime or threat of death or serious bodily harm to any person, or

(3) Anomalies that reveal a potential vulnerability to U.S. communications security. Communications for which the Attorney General or DIRNSA/CHCSS's waiver is sought should be forwarded to NSA/CSS, Attn: P02.

5.5. ~~(S-CCO)~~ Radio Communications with a Terminal in the UNITED STATES.

a. All radio communications that pass over channels with a terminal in the UNITED STATES must be processed through a computer scan dictionary or similar device unless those communications occur over channels used exclusively by a FOREIGN POWER.

b. International common-access radio communications that pass over channels with a terminal in the UNITED STATES [redacted] communications, may be processed without the use of a computer scan dictionary or similar device if necessary to determine whether a channel contains communications of FOREIGN INTELLIGENCE interest which NSA may wish to collect. Such processing may not exceed two hours without the specific prior written approval of the DDO and, in any event, shall be limited to the minimum amount of time necessary to determine the nature of communications on the channel and the amount of such communications that include FOREIGN INTELLIGENCE. Once it is determined that the channel contains sufficient communications of FOREIGN INTELLIGENCE interest to

warrant COLLECTION and exploitation to produce FOREIGN INTELLIGENCE, a computer scan dictionary or similar device must be used for additional processing.

c. Copies of all DDO written approvals made pursuant to 5.5.b. must be provided to the General Counsel and the Inspector General.

SECTION 6 – RETENTION

6.1. ~~(S-CCO)~~ Retention of Communications to, from or About U.S. PERSONS.

a. Except as otherwise provided in Annex A, Appendix 1, Section 4, communications to, from or about U.S. PERSONS that are intercepted by the USSS may be retained in their original or transcribed form only as follows:

(1) Unenciphered communications not thought to contain secret meaning may be retained for five years unless the DDO determines in writing that retention for a longer period is required to respond to authorized FOREIGN INTELLIGENCE requirements.

(2) Communications necessary to maintain technical data bases for cryptanalytic or traffic analytic purposes may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future FOREIGN INTELLIGENCE requirement. Sufficient duration may vary with the nature of the exploitation and may consist of any period of time during which the technical data base is subject to, or of use in, cryptanalysis. If a U.S. PERSON'S identity is not necessary to maintaining technical data bases, it should be deleted or replaced by a generic term when practicable.

b. Communications which could be disseminated under Section 7, below (i.e., without elimination of references to U.S. PERSONS) may be retained in their original or transcribed form.

6.2. ~~(S-CCO)~~ Access. Access to raw traffic storage systems which contain identities of U.S. PERSONS must be limited to SIGINT production personnel.

SECTION 7 – DISSEMINATION

7.1. ~~(C-CCO)~~ Focus of SIGINT Reports. All SIGINT reports will be written so as to focus solely on the activities of foreign entities and persons and their agents. Except as provided in Section 7.2., FOREIGN INTELLIGENCE information concerning U.S. PERSONS must be disseminated in a manner which does not identify the U.S. PERSON. Generic or general terms or phrases must be substituted for the identity (e.g., "U.S. firm" for the specific name of a U.S. CORPORATION or "U.S. PERSON" for the specific name of a U.S. PERSON). Files containing the identities of U.S. persons deleted from SIGINT reports will be maintained for a maximum period of one year and any requests from SIGINT customers for such identities should be referred to P02.

7.2. ~~(C-CCO)~~ Dissemination of U.S. PERSON Identities. SIGINT reports may include the identification of a U.S. PERSON only if one of the following conditions is met and a determination is made

by the appropriate approval authority that the recipient has a need for the identity for the performance of his official duties:

a. The U.S. PERSON has CONSENTED to the dissemination of communications of, or about, him or her and has executed the CONSENT form found in Annex H of this USSID, or

b. The information is PUBLICLY AVAILABLE (i.e., the information is derived from unclassified information available to the general public), or

c. The identity of the U.S. PERSON is necessary to understand the FOREIGN INTELLIGENCE information or assess its importance. The following nonexclusive list contains examples of the type of information that meet this standard:

(1) FOREIGN POWER or AGENT OF A FOREIGN POWER. The information indicates that the U.S. PERSON is a FOREIGN POWER or an AGENT OF A FOREIGN POWER.

(2) Unauthorized Disclosure of Classified Information. The information indicates that the U.S. PERSON may be engaged in the unauthorized disclosure of classified information.

(3) International Narcotics Activity. The information indicates that the individual may be engaged in international narcotics trafficking activities. (See Annex J of this USSID for further information concerning individuals involved in international narcotics trafficking).

(4) Criminal Activity. The information is evidence that the individual may be involved in a crime that has been, is being, or is about to be committed, provided that the dissemination is for law enforcement purposes.

(5) Intelligence TARGET. The information indicates that the U.S. PERSON may be the TARGET of hostile intelligence activities of a FOREIGN POWER.

(6) Threat to Safety. The information indicates that the identity of the U.S. PERSON is pertinent to a possible threat to the safety of any person or organization, including those who are TARGETS, victims or hostages of INTERNATIONAL TERRORIST organizations. Reporting units shall identify to P02 any report containing the identity of a U.S. PERSON reported under this subsection (6). Field reporting to P02 should be in the form of a CRITICOMM message (DDI XAO) and include the report date-time-group (DTG), product serial number and the reason for inclusion of the U.S. PERSON'S identity.

(7) Senior Executive Branch Officials. The identity is that of a senior official of the Executive Branch of the U.S. Government. In this case only the official's title will be disseminated. Domestic political or personal information on such individuals will be neither disseminated nor retained.

7.3. ~~(C-CCO)~~ Approval Authorities. Approval authorities for the release of identities of U.S. persons under Section 7 are as follows:

a. DIRNSA/CHCSS. DIRNSA/CHCSS must approve dissemination of:

(1) The identities of any senator, congressman, officer, or employee of the Legislative Branch of the U.S. Government.

(2) The identity of any person for law enforcement purposes.

b. Field Units and NSA Headquarters Elements. All SIGINT production organizations are authorized to disseminate the identities of U.S. PERSONS when:

(1) The identity is pertinent to the safety of any person or organization.

(2) The identity is that of a senior official of the Executive Branch.

(3) The U.S. PERSON has CONSENTED under paragraph 7.2.a. above.

c. DDO and Designees.

(1) In all other cases, U.S. PERSON identities may be released only with the prior approval of the Deputy Director for Operations, the Assistant Deputy Director for Operations, the Chief, P02, the Deputy Chief, P02, or, in their absence, the Senior Operations Officer of the National SIGINT Operations Center. The DDO or ADDO shall review all U.S. identities released by these designees as soon as practicable after the release is made.

(1) For law enforcement purposes involving narcotics related information, DIRNSA has granted to the DDO authority to disseminate U.S. identities. This authority may not be further delegated.

7.4. (U) Privileged Communications and Criminal Activity. All proposed disseminations of information constituting U.S. PERSON privileged communications (e.g., attorney/client, doctor/patient) and all information concerning criminal activities or criminal or judicial proceedings in the UNITED STATES must be reviewed by the Office of General Counsel prior to dissemination.

7.5. (U) Improper Dissemination. If the name of a U.S. PERSON is improperly disseminated, the incident should be reported to P02 within 24 hours of discovery of the error.

SECTION 8 – RESPONSIBILITIES

8.1. (U) Inspector General.
The Inspector General shall:

a. Conduct regular inspections and perform general oversight of NSA/CSS activities to ensure compliance with this USSID.

b. Establish procedures for reporting by Key Component and Field Chiefs of their activities and practices for oversight purposes.

c. Report to the DIRNSA/CHCSS, annually by 31 October, concerning NSA/CSS compliance with this USSID.

d. Report quarterly with the DIRNSA/CHCSS and General Counsel to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense (Intelligence Oversight).

APPROVED FOR PUBLIC RELEASE

8.2. (U) General Counsel. The General Counsel shall:

a. Provide legal advice and assistance to all elements of the USSS regarding SIGINT activities. Requests for legal advice on any aspect of these procedures should be sent by CRITICOMM to DDI XDI, or by NSA/CSS secure telephone 963-3121, or [redacted]

b. Prepare and process all applications for Foreign Intelligence Surveillance Court orders and requests for Attorney General approvals required by these procedures.

c. Advise the Inspector General in inspections and oversight of USSS activities.

d. Review and assess for legal implications as requested by the DIRNSA/CHCSS, Deputy Director, Inspector General or Key Components Chief, all new major requirements and internally generated USSS activities.

e. Advise USSS personnel of new legislation and case law that may affect USSS missions, functions, operations, activities, or practices.

f. Report as required to the Attorney General and the President's Intelligence Oversight Board and provide copies of such reports to the DIRNSA/CHCSS and affected agency elements.

g. Process requests from any DoD intelligence component for authority to use signals as described in Procedure 5, Part 5, of DoD 5240.1-R, for periods in excess of 90 days in the development, test, or calibration of ELECTRONIC SURVEILLANCE equipment and other equipment that can intercept communications.

8.3. (U) Deputy Director for Operations (DDO).
The DDO shall:

a. Ensure that all SIGINT production personnel understand and maintain a high degree of awareness and sensitivity to the requirements of this USSID.

b. Apply the provisions of this USSID to all SIGINT production activities. The DDO staff focal point for USSID 18 matters is P02 (use CRITICOMM DDI XAO).

c. Conduct necessary reviews of SIGINT production activities and practices to ensure consistency with this USSID.

d. Ensure that all new major requirements levied on the USSS or internally generated activities are considered for review by the General Counsel. All activities that raise questions of law or the proper interpretation of this USSID must be reviewed by the General Counsel prior to acceptance or execution.

8.4. (U) All Elements of the USSS. All elements of the USSS shall:

a. Implement this directive upon receipt.

b. Prepare new procedures or amend or supplement existing procedures as required to ensure adherence to this USSID. A copy of such procedures shall be forwarded to NSA/CSS, Attn: P02.

c. Immediately inform the DDO of any tasking or instructions that appear to require actions at variance with this USSID.

d. Promptly report to the NSA Inspector General and consult with the NSA General Counsel on all activities that may raise a question of compliance with this USSID.

SECTION 9 – DEFINITIONS

9.1. ~~(S-CCO)~~ AGENT OF A FOREIGN POWER means:

a. Any person, other than a U.S. PERSON, who:

(1) Acts in the UNITED STATES as an officer or employee of a FOREIGN POWER, or as a member of a group engaged in INTERNATIONAL TERRORISM or activities in preparation therefor; or

(2) Acts for, or on behalf of, a FOREIGN POWER that engages in clandestine intelligence activities in the UNITED STATES contrary to the interests of the UNITED STATES, when the circumstances of such person's presence in the UNITED STATES indicate that such person may engage in such activities in the UNITED STATES, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

b. Any person, including a U.S. PERSON, who:

(1) Knowingly engages in clandestine intelligence gathering activities for, or on behalf of, a FOREIGN POWER, which activities involve, or may involve, a violation of the criminal statutes of the UNITED STATES; or

(2) Pursuant to the direction of an intelligence service or network of a FOREIGN POWER, knowingly engages in any other clandestine intelligence activities for, or on behalf of, such FOREIGN POWER, which activities involve or are about to involve, a violation of the criminal statutes of the UNITED STATES; or

(3) Knowingly engages in sabotage or INTERNATIONAL TERRORISM, or activities that are in preparation therefor, for or on behalf of a FOREIGN POWER; or

(4) Knowingly aids or abets any person in the conduct of activities described in paragraphs 9.1.b.(1) through (3) or knowingly conspires with any person to engage in those activities.

c. For all purposes other than the conduct of ELECTRONIC SURVEILLANCE as defined by the Foreign Intelligence Surveillance Act (see Annex A), the phrase "AGENT OF A FOREIGN POWER" also means any person, including U.S. PERSONS outside the UNITED STATES, who are officers or employees of a FOREIGN POWER, or who act unlawfully for or pursuant to the direction of a FOREIGN POWER, or who are in contact with or acting in collaboration with an intelligence or security service of a FOREIGN POWER for the purpose of providing access to information or material classified by the UNITED STATES Government and to which the person has or has had access. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this provision,

APPROVED FOR PUBLIC RELEASE

absent evidence that the person is taking direction from or acting in knowing concert with a FOREIGN POWER.

9.2. ~~(S)~~ COLLECTION means intentional tasking or SELECTION of identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record.

9.3. (U) COMMUNICANT means a sender or intended recipient of a communication.

9.4. (U) COMMUNICATIONS ABOUT A U.S. PERSON are those in which the U.S. PERSON is identified in the communication. A U.S. PERSON is identified when the person's name, unique title, address, or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A mere reference to a product by brand name or manufacturer's name, e.g., "Boeing 707" is not an identification of a U.S. person.

9.5. (U) CONSENT, for SIGINT purposes, means an agreement by a person or organization to permit the USSS to take particular actions that affect the person or organization. An agreement by an organization with the National Security Agency to permit COLLECTION of information shall be deemed valid CONSENT if given on behalf of such organization by an official or governing body determined by the General Counsel, National Security Agency, to have actual or apparent authority to make such an agreement.

9.6. (U) CORPORATIONS, for purposes of this USSID, are entities legally recognized as separate from the persons who formed, own, or run them. CORPORATIONS have the nationality of the nation state under whose laws they were formed. Thus, CORPORATIONS incorporated under UNITED STATES federal or state law are U.S. PERSONS.

9.7. (U) ELECTRONIC SURVEILLANCE means:

a. In the case of an electronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is a party to the communication.

b. In the case of a nonelectronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is visibly present at the place of communication.

c. The term ELECTRONIC SURVEILLANCE does not include the use of radio direction finding equipment solely to determine the location of a transmitter.

9.8. ~~(S)~~ FOREIGN COMMUNICATION means a communication that has at least one COMMUNICANT outside of the UNITED STATES, or that is entirely among FOREIGN POWERS or between a FOREIGN POWER and officials of a FOREIGN POWER, but does not include communications intercepted by ELECTRONIC SURVEILLANCE directed at premises in the UNITED STATES used predominantly for residential purposes.

9.9. (U) FOREIGN INTELLIGENCE means information relating to the capabilities, intentions, and activities of FOREIGN POWERS, organizations, or persons, and for purposes of this USSID includes both positive FOREIGN INTELLIGENCE and counterintelligence.

9.10. (U) FOREIGN POWER means:

a. A foreign government or any component thereof, whether or not recognized by the UNITED STATES,

b. A faction of a foreign nation or nations, not substantially composed of UNITED STATES PERSONS,

c. An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments,

d. A group engaged in INTERNATIONAL TERRORISM or activities in preparation therefor,

e. A foreign-based political organization, not substantially composed of UNITED STATES PERSONS, or

f. An entity that is directed and controlled by a foreign government or governments.

9.11. (U) INTERCEPTION means the acquisition by the USSS through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form, but does not include the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signal.

9.12. (U) INTERNATIONAL TERRORISM means activities that:

a. Involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the UNITED STATES or of any State, or that would be a criminal violation if committed within the jurisdiction of the UNITED STATES or any State, and

b. Appear to be intended:

(1) to intimidate or coerce a civilian population,

(2) to influence the policy of a government by intimidation or coercion, or

(3) to affect the conduct of a government by assassination or kidnapping, and

c. Occur totally outside the UNITED STATES, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

9.13. (U) PUBLICLY AVAILABLE INFORMATION means information that has been published or broadcast for general public consumption, is available on request to a member of the general public, has been seen or heard by a casual observer, or is made available at a meeting open to the general public.

9.14. ~~(C)~~ SELECTION, as applied to manual and electronic processing activities, means the intentional insertion of a [redacted] telephone number, [redacted] into a computer scan dictionary or manual scan guide for the purpose of identifying messages of interest and isolating them for further processing.

9.15. ~~(C)~~ SELECTION TERM means the composite of individual terms used to effect or defeat SELECTION of particular communications for the purpose of INTERCEPTION. It comprises the entire term or series of terms so used, but not any segregable term contained therein. It applies to both electronic and manual processing.

9.16. (U) TARGET, OR TARGETING: See COLLECTION.

9.17. (U) UNITED STATES, when used geographically, includes the 50 states and the District of Columbia, Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, the Northern Mariana Islands, and any other territory or possession over which the UNITED STATES exercises sovereignty.

9.18. ~~(C)~~ UNITED STATES PERSON:

a. A citizen of the UNITED STATES,

b. An alien lawfully admitted for permanent residence in the UNITED STATES,

c. Unincorporated groups and associations a substantial number of the members of which constitute a. or b. above, or

d. CORPORATIONS incorporated in the UNITED STATES, including U.S. flag nongovernmental aircraft or vessels, but not including those entities which are openly acknowledged by a foreign government or governments to be directed and controlled by them.

e. The following guidelines apply in determining whether a person is a U.S. PERSON:

(1) A person known to be currently in the United States will be treated as a U.S. PERSON unless that person is reasonably identified as an alien who has not been admitted for permanent residence or if the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is not a U.S. PERSON.

(2) A person known to be currently outside the UNITED STATES, or whose location is not known, will not be treated as a U.S. PERSON unless such person is reasonably identified as such or the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is a U.S. PERSON.

(3) A person known to be an alien admitted for permanent residence may be assumed to have lost status as a U.S. PERSON if the person leaves the UNITED STATES and it is known that the person is not in compliance with the administrative formalities provided by law (8 U.S.C. Section 1203) that enable such persons to reenter the UNITED STATES without regard to the provisions of law that would otherwise restrict an alien's entry into the UNITED STATES. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

(4) An unincorporated association whose headquarters are located outside the UNITED STATES may be presumed not to be a U.S. PERSON unless the USSS has information indicating that a substantial number of members are citizens of the UNITED STATES or aliens lawfully admitted for permanent residence.

APPROVED FOR PUBLIC RELEASE

(5) CORPORATIONS have the nationality of the nation-state in which they are incorporated. CORPORATIONS formed under U.S. federal or state law are thus U.S. persons, even if the corporate stock is foreign-owned. The only exception set forth above is CORPORATIONS which are openly acknowledged to be directed and controlled by foreign governments. Conversely, CORPORATIONS incorporated in foreign countries are not U.S. PERSONS even if that CORPORATION is a subsidiary of a U.S. CORPORATION.

(6) Nongovernmental ships and aircraft are legal entities and have the nationality of the country in which they are registered. Ships and aircraft fly the flag and are subject to the law of their place of registration.

APPROVED FOR PUBLIC RELEASE

~~TOP SECRET//STLW//HCS/COMINT//ORCON/NOFORN~~

~~TOP SECRET//STLW//SI//ORCON/NOFORN~~

No. OP 2008-0009

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

OFFICE OF THE INSPECTOR GENERAL

~~(S//NF)~~ REVIEW OF THE PARTICIPATION OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE IN THE PRESIDENT'S SURVEILLANCE PROGRAM

July 2, 2009

ROSLYN A. MAZER
INSPECTOR GENERAL

Copy No.

CL BY: 2385885
CL
REASON: 1.4(C),(G)
DECL ON: 20340218
DRV FROM: MIS S-06,
ODNI COM T-08

This page intentionally left blank.

APPROVED FOR PUBLIC RELEASE

(U) TABLE OF CONTENTS

		PAGE
I.	(U) EXECUTIVE SUMMARY	2
II.	(U) INTRODUCTION	3
III.	(U) SCOPE AND METHODOLOGY	3
IV.	(U) DISCUSSION OF FINDINGS	4
	A. (U) Initial Response by the President and Congress to the Terrorist Attacks of September 11, 2001 (U)	4
	B. ~~(TS//STLW//SI//OC/NF)~~ ODNI Role in Preparing Threat Assessments in Support of the Program	6
	C. ~~(TS//STLW//SI//OC//NF)~~ NCTC Use of the Program to Support Counterterrorism Analysis	10
	D. [redacted]	12
	E. ~~(TS//STLW//SI//OC/NF)~~ NCTC Role in Identifying Program Targets or Tasking Collection	13
	F. ~~(S/NF)~~ ODNI Oversight of the Program	13
V.	(U) CONCLUSION	16
VI.	(U) APPENDIX – STRUCTURE OF THE ODNI - 2005	17

This page intentionally left blank.

~~(S/NF)~~ REVIEW OF THE PARTICIPATION OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE IN THE PRESIDENT'S SURVEILLANCE PROGRAM

I. (U) EXECUTIVE SUMMARY

~~(TS//STLW//SI//OC/NF)~~ The Office of Inspector General (OIG), Office of the Director of National Intelligence (ODNI), was one of five Intelligence Community Inspectors General that conducted a review of their agency's participation in the President's Surveillance Program (hereafter "the Program"), a top secret National Security Agency (NSA) electronic surveillance activity undertaken at the direction of the President. The Program became operational on October 4, 2001, three weeks after the deadly terrorist attacks of September 11, 2001. The review examined the ODNI's involvement in the Program from the period beginning with the stand-up of the ODNI in April 2005 through the termination of the Program in January 2007.

~~(TS//STLW//SI//OC/NF)~~ The ODNI's primary role in the Program was the preparation of the threat assessments that summarized the al Qaeda terrorist threat to the United States and were used to support the periodic reauthorization of the Program. That role began in April 2005, shortly after the ODNI stand-up and contemporaneous with the arrival of General Michael Hayden as the first Principal Deputy Director of National Intelligence (PDDNI). Prior to his ODNI appointment, Hayden was Director of NSA. In April 2005, ODNI personnel in the National Counterterrorism Center (NCTC) began to prepare the first of 12 Program threat assessments. In coordination with the Department of Justice (DOJ), then Director of National Intelligence (DNI) John Negroponte or PDDNI Hayden approved 12 ODNI-prepared threat assessments over an 18-month period. Once approved by the DNI or PDDNI, the Program threat assessments were reviewed and approved by the Secretary of Defense, and were subsequently used by DOJ, NSA, and White House personnel in support of the Program reauthorization. In addition to the preparation of the threat assessments, we found that NCTC used Program information in producing analytical products that were distributed to senior IC community officials and analysts. [redacted]

~~(TS//STLW//SI//OC/NF)~~ During the review, we made several related findings and observations. We learned that the ODNI usage of Program-derived information in ODNI intelligence products was consistent with the standard rules and procedures for handling NSA intelligence. We learned that ODNI personnel were not involved in nominating specific targets for collection through the Program. While ODNI personnel were identified as having contact [redacted] regarding the Program, we found that those communications were limited in frequency and scope. We also found that the ODNI intelligence oversight components -- the Civil Liberties Protection Officer (CLPO), Office of General Counsel (OGC), and the OIG -- had little involvement in oversight of the Program and had limited opportunity to participate in Program oversight due to delays in ODNI oversight personnel being granted access to the

Program and temporary resource limitations attendant to the stand-up of the ODNI. Finally, we found that the 2008 amendments to Executive Order 12333 and the current ODNI staffing levels provide the ODNI oversight components with sufficient resources and authority to fulfill their current oversight responsibilities, assuming timely notification.

II. (U) INTRODUCTION

~~(TS//STLW//SI//OC/NF)~~ *The Foreign Intelligence Surveillance Act Amendments Act of 2008*, Pub L. No. 110-261, 122 Stat. 2438 (hereafter "FISA Amendments Act") required the IGs of the DOJ, ODNI, NSA, Department of Defenses (DOD), and any other element of the intelligence community that participated in the President's Surveillance Program to conduct a comprehensive review of the Program.[1] The FISA Amendments Act defined the "President's Surveillance Program" as the "intelligence activity involving communications authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005." In response to this tasking, the IGs of the following five agencies were identified as having a role in Program review: DOJ, ODNI, NSA, DOD, and the Central Intelligence Agency (CIA).

~~(S//NF)~~ The participating IGs organized the review in a manner where each OIG conducted a review of its own agency's involvement in the Program. CIA IG John Helgerson was initially designated by the IGs to coordinate the review and oversee the preparation of an interim report due within 60 days after the enactment of the Act, and a later final report due not later than 1 year after the enactment of the Act.[2] Because of IG Helgerson's recent retirement, DOJ IG Glenn Fine was selected to coordinate the preparation of the final report. This report contains the results of the ODNI OIG review.

III. (U) SCOPE AND METHODOLOGY

~~(TS//STLW//SI//OC/NF)~~ We sought to identify the role of the ODNI in implementing the Program beginning with the stand-up of the ODNI in April 2005 through the Program's termination in January 2007. This review examined the:

A. Role of the ODNI and its component the National Counterterrorism Center (NCTC) in drafting and coordinating the threat assessments that supported the periodic reauthorization of the Program;

---

[1] ~~(S//NF)~~ The Program is also known within the Intelligence Community by the cover term STELLARWIND. The Program is a Top Secret/Sensitive Compartmented Information (SCI) program.

[2] (U) The participating IGs submitted an interim report, dated September 10, 2008, to the Chairman and Ranking member of the Senate Select Committee on Intelligence (SSCI) and a revised interim report, dated November 24, 2008, to the Chairman and Ranking member of the House of Representatives Permanent Select Committee on Intelligence (HPSCI).

B. NCTC's use of Program information to support counterterrorism analysis;

C. NCTC's role in identifying Program targets and tasking Program collection;

D. [redacted] and

F. Role of the ODNI in providing compliance oversight of the Program.

~~(TS//STLW//SI//OC/NF)~~ During the review, we interviewed 23 current or former ODNI officials and employees involved in the Program. The ODNI personnel we interviewed were cooperative and helpful. Our interviews included the following ODNI senior officials:

John Negroponte, former Director of National Intelligence
Michael McConnell, former Director of National Intelligence
Michael V. Hayden, former Principal Deputy Director of National Intelligence
Ronald Burgess, former Acting Principal Deputy Director of National Intelligence
David R. Shedd, Deputy Director of National Intelligence for Policy, Plans, and Requirements
Alexander W. Joel, Civil Liberties Protection Officer
Edward Maguire, former Inspector General
Benjamin Powell, former General Counsel
Corin Stone, Deputy General Counsel and Acting General Counsel
Joel Brenner, former National Counterintelligence Executive[3]
John Scott Redd, former NCTC Director
Michael Leiter, NCTC Director

~~(S//NF)~~ In addition to the interviews noted above, we reviewed Program-related documents made available by the NSA OIG, the DOJ OIG, and the ODNI OGC.

IV. (U) DISCUSSION OF FINDINGS

~~(TS//STLW//SI//OC/NF)~~ The following discussion contains our findings regarding the topics identified above. First, we briefly describe the terrorist attacks of September 11, 2001, and the initial government response to the attacks, including the authorization of the President's Surveillance Program. Next, we discuss the ODNI and NCTC role in implementing the Program. Finally, we set forth our conclusions and observations.

A. (U) Initial Response by the President and Congress to the Terrorist Attacks of September 11, 2001

(U) The devastating al Qaeda terrorist attacks against the United States quickly triggered an unprecedented military and intelligence community response to protect the

[3] (U) Brenner was the NSA Inspector General before joining the ODNI.

country from additional attacks. The following quote describes the initial terrorist attacks and the intended al Qaeda goal to deliver a decapitating strike against our political institutions.

> (U) On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial airliners, each carefully selected to be fully loaded with jet fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners were targeted at the Nation's financial center in New York and were deliberately flown into the Twin Towers of the World Trade Center. The third was targeted at the headquarters of the Nation's Armed Forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was evidently the White House or the Capitol, strongly suggesting that its intended mission was to strike a decapitation blow on the Government of the United States – to kill the President, the Vice President, or Members of Congress. The attacks of September 11th resulted in approximately 3,000 deaths – the highest single-day death toll from hostile foreign attacks in the Nation's history.[4]

(U) On September 14, 2001, in response to the attacks, the President issued a *Declaration of National Emergency by Reason of Certain Terrorist Attacks* stating that "(a) national emergency exists by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and continuing immediate threat of further attacks on the United States."[5]

(U) On September 18, 2001, by an overwhelming majority in both the Senate and House of Representatives, a joint resolution was passed that authorized the use of United States military force against those responsible for the terrorist attacks launched against the United States. The joint resolution, also known as the *Authorization for Use of Military Force (AUMF)*, is often cited by White House and DOJ officials as one of the principal legal authorities upon which the Program is based. In relevant part, the AUMF provides:[6]

> (a) IN GENERAL – That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organization or persons, in order to

---

[4] (U) This summary of the events of September 11, 2001, was prepared by DOJ personnel and is set forth in the unclassified DOJ "White Paper" entitled *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, dated January 19, 2006.

[5] (U) Proclamation 7463, 66 Fed. Reg. No. 181, September 14, 2001.

[6] (U) *Authorization for Use of Military Force*, Section 2(a), Pub. L. No. 170-40, 115 Stat. 224, September 18, 2001.

prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

~~(TS//STLW//SI//OC/NF)~~ On October 4, 2001, three days before the start of overt military action against the al Qaeda and Taliban terrorist camps, the President authorized the Secretary of Defense to implement the President's Surveillance Program.[7] The Program, a closely held top-secret NSA electronic surveillance project, authorized the Secretary of Defense to employ within the United States the capabilities of the DOD, including but not limited to the signals intelligence capabilities of the NSA, to collect international terrorism-related foreign intelligence information under certain specified circumstances. Each Program reauthorization was supported by a written threat assessment, approved by a senior Intelligence Community official, that described the threat of a terrorist attack against the United States.

(U) On October 7, 2001, in a national television broadcast, the President announced the start of military operations against al Qaeda and Taliban terrorist camps in Afghanistan.[8]

~~(TS//STLW//SI//OC/NF)~~ On April 22, 2005, the ODNI began operations as the newest member of the Intelligence Community. The ODNI was created, in part, in response to the findings of the *Independent National Commission on Terrorist Attacks Upon the United States* (hereafter 9/11 Commission) that recommended the creation of a national "Director of National Intelligence" to oversee and coordinate the planning, policy, and budgets of the Intelligence Community.[9] In late April 2005, ODNI personnel began to prepare the threat assessments used in the periodic reauthorization of the Program. In June 2005, ODNI officials began to approve the threat assessments.

B. ~~(TS//STLW//SI//OC/NF)~~ ODNI Role in Preparing Threat Assessments in Support of the Program Reauthorizations

~~(TS//STLW//SI//OC/NF)~~ Prior to the ODNI's involvement in the Program, the Program was periodically reauthorized approximately every 30 to 45 days pursuant to a reauthorization process overseen by DOJ, NSA, and White House personnel. Each reauthorization relied, in part, on a written threat assessment approved by a senior Intelligence Community official that described the current threat of a terrorist attack against the United States and contained the approving official's recommendation regarding the need to reauthorize the Program. Before the ODNI's involvement in the

---

[7] ~~(TS//STLW//SI//OC/NF)~~ The NSA materials we reviewed identified October 4, 2001, as the date of the first Program authorization.

[8] (U) The CNN.com webpage article entitled *President announces opening of attack*, dated, October 7, 2001, provides a summary of the President's announcement and describes the national television broadcast.

[9] (U) While the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) that created the ODNI was signed by the President on December 17, 2004, the actual ODNI stand-up occurred months later. The official ODNI history, *A Brief History of the ODNI's Founding*, sets April 22, 2005, as the date when the ODNI commenced operations.

Program, every threat assessment prepared by the Intelligence Community in support of the Program reauthorization identified the threat of a terrorist attack against the United States and recommended that the Program be reauthorized. Accordingly, the Program was regularly reauthorized during the approximately 3-year period prior to the involvement of the ODNI. During that period, the Director of Central Intelligence or his designee approved 31 threat assessments in support of the reauthorization of the Program.

~~(TS//STLW//SI//OC/NF)~~ In reviewing the circumstances that led to the decision to transfer responsibility for preparing the Program threat assessments to the ODNI, we found that the ODNI does not have identifiable records regarding that decision. Senior ODNI officials involved with the Program told us that after the merger of the Terrorist Threat Integration Center (TTIC) into the NCTC, and the later incorporation of NCTC into the ODNI, it made sense for the ODNI to take responsibility for preparing the Program threat assessments as both TTIC and NCTC previously handled that task. Former PDDNI Hayden told us that the primary reason that the ODNI become involved in the Program was the statutory creation of the new DNI position as the senior Intelligence Community advisor to the President. When Ambassador Negroponte was confirmed as the first DNI, Hayden and other senior intelligence officials believed that DNI Negroponte, as the President's new senior intelligence advisor, should make the Intelligence Community's recommendation to the President regarding the need to renew the Program. Hayden commented that the new DNI's involvement in this important intelligence program enhanced the DNI's role as the leader of the Intelligence Community and gave immediate credibility to the ODNI as a new intelligence agency.

~~(TS//STLW//SI//OC/NF)~~ Once the ODNI became involved in the Program, the preparation and approval of the threat assessments became the ODNI's primary Program role.[10] Beginning in April 2005, and continuing at about 30 to 45 day intervals until the Program's termination in January 2007, ODNI personnel prepared and approved 12 written threat assessments in support of the periodic reauthorization of the Program. We found that the ODNI threat assessments were drafted by experienced NCTC personnel who prepared the documents following an established DOJ format used in earlier Program reauthorizations. NCTC analysts prepared the threat assessments in a memorandum format, usually 12 to 14 pages in length. Senior ODNI and NCTC officials told us that each threat assessment was intended to set forth the ODNI's view regarding the current threat of an al Qaeda attack against the United States and to provide the DNI's recommendation whether to continue the Program. NCTC personnel involved in preparing the threat assessments told us that the danger of a terrorist attack described in the threat assessments was sobering and "scary," resulting in the threat assessments becoming known by ODNI and Intelligence Community personnel involved in the Program as the "scary memos."

[10] ~~(TS//STLW//SI//OC/NF)~~ The joint interim report prepared by the participating IGs notified congressional oversight committees that the review would examine the ODNI's involvement in preparing "threat assessments and legal certifications" submitted in support of the Program. Because we did not identify any ODNI officials executing a legal certification, we treated our review of the legal certifications to be the same as the review of the threat assessments. The Attorney General made legal certifications in support of the Program that are addressed in the DOJ OIG report.

~~(TS//STLW//SI//OC/NF)~~ During interviews, ODNI personnel said they were aware that the threat assessments were relied upon by DOJ and the White House as the basis for continuing the Program and further understood that if a threat assessment identified a threat against the United States, the Program was likely to be reauthorized. NCTC analysts also said that on a less frequent basis they prepared a related document that set forth a list of al Qaeda-affiliated groups that they understood were targets of the Program. Both the threat assessments and the less frequent list of al Qaeda-affiliated groups underwent the same ODNI approval process.

~~(TS//STLW//SI//OC/NF)~~ We examined the ODNI process for preparing the Program documents, particularly the threat assessments, and found that the documents were drafted by experienced NCTC analysts under the supervision of the NCTC Director and his management staff, who were ultimately responsible for the accuracy of the information in the documents. We determined that the ODNI threat assessments were prepared using evaluated intelligence information chosen from a wide-variety of Intelligence Community sources. ODNI personnel told us that during the period when the ODNI prepared the threat assessments, the Intelligence Community had access to fully evaluated intelligence that readily supported the ODNI assessments that al Qaeda terrorists remained a significant threat to the United States.

~~(TS//STLW//SI//OC/NF)~~ Once the ODNI threat assessments were approved within NCTC and by the NCTC Director, the documents were forwarded through an established approval chain to senior ODNI personnel who independently satisfied themselves that the documents were accurate, properly prepared, and in the appropriate format. Throughout the ODNI preparation and approval process, the threat assessments were also subject to varying degrees of review and comment by DOJ and OGC attorneys, including then General Counsel Benjamin Powell and Deputy General Counsel Corin Stone. Powell said his review of the threat assessments was not a legal review, but was focused on spotting issues that might merit further review or analysis. Powell said he relied on DOJ to conduct the legal review. Once the draft threat assessments were subjected to this systematic and multi-layered management and legal review, the documents were provided to the DNI or PDDNI for consideration and, if appropriate, approval. Overall, we found the process used by the ODNI to prepare and obtain approval of the threat assessments was straightforward, reasonable, and consistent with the preparation of other documents requiring DNI or PDDNI approval.

~~(TS//STLW//SI//OC/NF)~~ Negroponte told us that because of time-sensitive issues present in 2005 relating to the ongoing ODNI start-up as a new agency and other Intelligence Community matters requiring his attention, he tasked his deputy, then PDDNI Hayden, to oversee the ODNI approval of the threat assessments and related documents. Negroponte told us that when making this decision, he was aware of Hayden's prior experience with the Program during Hayden's earlier assignment as Director of NSA. In June 2005, shortly after his arrival at ODNI, Hayden received and approved the first ODNI threat assessment. Hayden later approved the next six ODNI threat assessments. After Hayden left the ODNI in May 2006 to become Director of CIA, Negroponte approved the next five ODNI threat assessments, including a December

2006 threat assessment used in the final reauthorization of the Program. In total, Negroponte and Hayden approved 12 ODNI threat assessments prepared in support of the Program reauthorizations.[11]

~~(TS//STLW//SI//OC/NF)~~ In discussing the ODNI process used to prepare and approve the threat assessments, Negroponte told us he was "extremely satisfied" with the quality and content of the threat assessments provided for his approval. He did not recall any inaccuracies or problems relating to preparation of the ODNI threat assessments. Negroponte said the al Qaeda threat information described in the Program threat assessments was consistent with the terrorism threat information found in *The President's Daily Briefing* and other senior-level Intelligence Community products he had read. Hayden had a similar view. Negroponte and Hayden separately told us that when they approved the threat assessments, credible intelligence was readily available to the Intelligence Community that demonstrated the ongoing and dangerous al Qaeda terrorist threat to the United States. Similarly, Negroponte and Hayden each told us that the nature and scope of the al Qaeda terrorist threat to the United States was well documented and easily supported the ODNI threat assessments used in the Program reauthorizations.

~~(TS//STLW//SI//OC/NF)~~ Because of questions raised in the media about the legal basis for the Program, we asked the ODNI personnel involved in the preparation or approval of the threat assessments about their concerns, if any, regarding the legal basis for the Program. We found that ODNI personnel involved in the Program generally understood that the Program had been in operation for several years and was approved by senior Intelligence Community and DOJ officials. During our interviews, ODNI officials told us they were satisfied with the legal basis for the Program, primarily because of their knowledge that the Attorney General and senior DOJ attorneys had personally approved the Program and remained directly involved in the Program reauthorization process. We did not identify any ODNI personnel who believed that the program was unlawful.

~~(TS//STLW//SI//OC/NF)~~ Former ODNI General Counsel Powell told us that after his Program briefings in early 2006, he had questions regarding the DOJ description of the legal authority for the Program but lacked the time to conduct his own legal review of the issue given the many time-sensitive ODNI legal issues that required his attention. Powell said he understood the rationale of DOJ's legal opinion that the Program was lawful and described the DOJ opinion as a "deeply complex issue" with "legal scholarship on both sides." Powell said he recognized that he was a latecomer to a complex legal issue that was previously and continuously approved by DOJ, personally supported by the Attorney General, and was being transitioned to judicial oversight – an idea he strongly supported. Powell said he relied on the DOJ legal opinion regarding the Program and directed his efforts to supporting the Program's transition to judicial oversight under traditional FISA, the 2007 Protect America Act, and the subsequent FISA Amendments Act of 2008.

---

[11] ~~(TS//STLW//SI//OC/NF)~~ The DNI and PDDNI together approved 12 of the 43 threat assessments used in support of the Program reauthorizations. CIA officials approved the other 31 threat assessments.

~~(TS//STLW//SI//OC/NF)~~ Negroponte recalled having regular contact with senior NSA and DOJ officials who raised no legal concerns to him about the Program. He said he remembered attending a Program-related meeting that included members of the FISA Court who did not raise any legal concerns to him about the authority for the Program and seemed generally supportive of the Program. Negroponte also recalled attending meetings in which the Program was briefed to congressional leadership who not did raise legal concerns to him. Overall, the direct involvement of DOJ and other senior Intelligence Community officials in the Program resulted in Negroponte and other ODNI personnel having few, if any, concerns about the legal basis for the Program.

C. ~~(TS//STLW//SI//OC/NF)~~ NCTC Use of Program Information to Support Counterterrorism Analysis

~~(TS//STLW//SI//OC/NF)~~ The Program information was closely held within the ODNI and was made available to no more than 15 NCTC analysts for review and, if appropriate, use in preparing NCTC analytical products.[12] Generally, the NCTC analysts approved for access received the Program information in the form of finished NSA intelligence products. [redacted] The NCTC analysts said the Program information was subject to stringent security protections [redacted] The NCTC analysts told us they received training regarding proper handling of NSA intelligence. They said they handled the NSA intelligence, including Program information, consistent with the standard rules and procedures for handling NSA intelligence information, including the minimization of U.S. person identities.

~~(TS//STLW//SI//OC/NF)~~ Hayden told us that during his tenure as Director of NSA, he sought to disseminate as much Program information as possible to the Intelligence Community [redacted]

~~(TS//STLW//SI//OC/NF)~~ During our review, NCTC analysts told us they often did not know if the NSA intelligence available to them was derived from the Program. [redacted]

[12] ~~(TS//STLW//SI//OC/NF)~~ The number of NCTC analysts read into the Program ranged from 5 to 15 analysts.

[redacted] On those occasions when the NCTC analysts knew that a particular NSA intelligence product was derived from the Program, the analysts said they reviewed the Program information in the same manner as other NSA intelligence products and, if appropriate, incorporated the Program information into analytical products being prepared for the DNI and other senior intelligence officials. They identified the *President's Terrorism Threat Report* and the *Senior Executive Terrorism Report* as examples of the types of finished intelligence products that would, at times, contain Program information.

~~(TS//STLW//SI//OC/NF)~~ NCTC analysts with Program access said they had broad access to a wide variety of high quality and fully evaluated terrorism related intelligence. In particular, NCTC analysts told us that by virtue of their NCTC assignments, they had access to some of the most sensitive and valuable terrorism intelligence available to the Intelligence Community. NCTC analysts characterized the Program information as being a useful tool, but also noted that the Program information was only one of several valuable sources of information available to them from numerous collection sources and methods. During interviews, NCTC analysts and other ODNI personnel described the Program information as "one tool in the tool box," "one arrow in the quiver," or in other similar phrases to connote that the Program information was not of greater value than other sources of intelligence. The NCTC analysts we interviewed said they could not identify specific examples where the Program information provided what they considered time-sensitive or actionable intelligence, but they generally recalled attending meetings in which the benefits of the Program were discussed. [redacted] The NCTC analysts uniformly told us that during the period when NCTC prepared the threat assessment memoranda, the intelligence demonstrating the al Qaeda threat to the United States was overwhelming and readily available to the Intelligence Community.

~~(TS//STLW//SI//OC/NF)~~ When asked about the value of the Program, Hayden said "without the Program as a skirmish line you wouldn't know what you don't know." He explained that by using the Program to look at a "quadrant of communications" the Intelligence Community was able to assess the threat arising from those communications, which allowed Intelligence Community leaders to make valuable judgments regarding the allocation of national security resources. He said looking at the terrorist threat in this manner was similar to soldiers on a combat patrol who look in all directions for the threat and assign resources based on what they learn. Hayden said that NSA General Counsel Vito Potenza often described the Program as an "early warning system" for terrorist threats, which Hayden thought was an accurate description of the Program. Hayden told us the Program was extremely valuable in protecting the United States from an al Qaeda terrorist attack. Hayden cited [redacted].

APPROVED FOR PUBLIC RELEASE

[redacted] as examples where the Program information was effectively used to disrupt al Qaeda operatives.[13]

D. [redacted]

[redacted]

13 [redacted]

[redacted]

E. ~~(TS//STLW//SI//OC/NF)~~ No NCTC Role in Identifying Program Targets and Tasking Collection

~~(TS//STLW//SI//OC/NF)~~ We did not identify any information that indicated that ODNI or NCTC personnel were involved in identifying or nominating targets for collection within the Program. ODNI personnel told us that ODNI and NCTC are non-operational elements of the Intelligence Community and were not involved in nominating targets for Program collection.

F. ~~(S/NF)~~ ODNI Oversight of the Program

~~(TS//STLW//SI//OC/NF)~~ We examined the role of the ODNI oversight components -- CLPO, OIG, and OGC -- in providing compliance oversight for the Program. We found that while the Program was subject to oversight by the NSA OIG, the ODNI oversight components had a limited role in providing oversight for the Program. During the review, we learned that within the first year of the Program, then NSA Director Hayden obtained White House approval allowing the NSA IG and designated NSA OIG officials to be read into the Program to provide compliance oversight for the Program. In furtherance of the NSA oversight program, the NSA IG provided compliance reports and briefings to the NSA Director, NSA General Counsel, and cleared White House personnel, including the Counsel to the President.[16]

~~(TS//STLW//SI//OC/NF)~~ In reviewing the ODNI oversight role regarding the Program, we found that the ODNI oversight components had limited involvement in oversight of the Program. We found that the opportunity for the ODNI to participate in Program oversight was limited by the fact that ODNI oversight personnel were not

[redacted]

[15] ~~(TS//STLW//SI//OC/NF)~~ [redacted]

[16] ~~(S//NF)~~ According to the General Counsel to the President's Intelligence Oversight Board (IOB), the IOB members and staff were not read into the Program and did not receive compliance reports from the NSA IG.

granted timely access to the Program by the White House personnel responsible for approving access. In addition, we found that the newly formed ODNI oversight offices were in varying stages of agency stand-up and lacked the necessary experienced staff and resources to effectively participate in oversight of the Program.

~~(TS//STLW//SI//OC/NF)~~ For example, General Counsel Powell received Program access after his arrival in January 2006, but his predecessor, then Acting General Counsel Corin Stone, was not read into the Program until a few days before Powell in January 2006, several months after the Program became operational within ODNI and only after she had read about the Program in a December 2005 newspaper article.[17] Similarly, CLPO Alexander Joel, who is responsible for reviewing the privacy and civil liberties implications of intelligence activities, requested but did not receive Program access until October 2006, shortly before the Program terminated.[18] Joel told us that Negroponte and Hayden supported his request for Program access, but White House staff delayed approval for several months. Joel said that while waiting for approval of his Program access, Hayden gave him some insight about the Program that did not require the disclosure of compartmented information. Joel found this information helpful in planning his later review. Finally, then ODNI Inspector General Edward Maguire and his oversight staff did not obtain Program access until 2008, long after the Program had terminated.[19]

~~(TS//STLW//SI//OC/NF)~~ Once read into the Program, Powell and Joel were provided with reasonable access to NSA compliance reports and briefings relating to the NSA OIG oversight program. Powell told us that he was satisfied that the NSA IG provided a reasonable degree of Program oversight. Similarly, Joel said he believed that he had received full disclosure regarding the NSA oversight program and found the NSA oversight effort to be reasonable.

~~(TS//STLW//SI//OC/NF)~~ We also learned that the members of the President's Privacy and Civil Liberties Oversight Board (PCLOB) reviewed the Program, in part, in association with Joel.[20] The PCLOB review was contemporaneous with Joel's review

---

[17] (U//~~FOUO~~) Powell was appointed General Counsel in January 2006 and served in that position as a recess appointment until his Senate confirmation in April 2006. Prior to his appointment, Powell was an Associate Counsel to the President and Special Assistant to the President where he worked on initiatives related to the Intelligence Community. However, Powell was not read into the Program while serving at the White House.

[18] (U//~~FOUO~~) Joel is the Civil Liberties Protection Officer (CLPO) with the responsibility for ensuring that the protection of privacy and civil liberties is incorporated in the policies and procedures of the Intelligence Community. The CLPO responsibilities are set forth in the Section 103d of *Intelligence Reform and Terrorism Prevention Act of 2004.*

[19] ~~(S//NF)~~ While OIG personnel were not read into the Program until 2008, OIG officials were alerted to the existence of the NSA collection program through a December 2005 newspaper report. Shortly after that report, the NSA IG told ODNI OIG officials that the NSA OIG was conducting oversight of that NSA program. PDDNI Hayden also told IG Maguire that the NSA program was subject to NSA OIG oversight.

[20] (U) The PCLOB was created by the *Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)*, which requires the Board to "ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism (P.L. 108-458, 2004).

and resulted in an independent and generally favorable finding regarding the NSA implementation of the Program. After the PCLOB review, a PCLOB board member published an editorial article, in part, quoted below, that summarized his observations regarding the NSA effort in implementing the Program.

> There were times, including when the Board was "read into" and given complete access to the operation of the Terrorist Surveillance Program that I wondered whether the individuals doing this difficult job on behalf of all of us were not being too careful, too concerned, about going over the privacy and liberties lines – so concerned, with so many internal checks and balances, that they could miss catching or preventing the bad guys from another attack. And I remember walking out of these briefing sessions in some dark and super-secret agency with the thought: I wish the American people could meet these people and observe what they are doing.[21]

~~(S//NF)~~ In sum, the ODNI oversight components had limited and belated involvement in the oversight of the Program. However, once read into the Program, Powell and Joel determined that the Program was subject to reasonable oversight by the NSA OIG. Moreover, the initial White House delay in granting ODNI oversight personnel access to the Program occurred prior to the 2008 revision to Executive Order (EO) 12333, which expressly grants ODNI oversight components broad access to any information necessary to performing their oversight duties. In particular, EO 12333 provides in relevant part that:

> Section 1.6 *Heads of Elements of the Intelligence Community*. The heads of elements of the Intelligence Community shall:
>
> (h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy and civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their duties.

~~(TS//STLW//SI//OC/NF)~~ EO 12333, as amended, clarifies and strengthens the ODNI's ability to provide compliance oversight. In light of the recent change to EO 12333, and with current staffing, we believe that ODNI's oversight components have sufficient resources and authority to perform their responsibilities to conduct oversight of closely held intelligence activities, assuming timely notification.

---

[21] (U) The quote is taken from a May 5, 2007, article by former PCLOB member Lanny Davis, entitled, "*Why I Resigned From The President's Privacy and Civil Liberties Oversight Board – And Where We Go From Here.*" The article was published on webpage of The Huffington Post, www.huffingtonpost.com.

V. (U) CONCLUSION

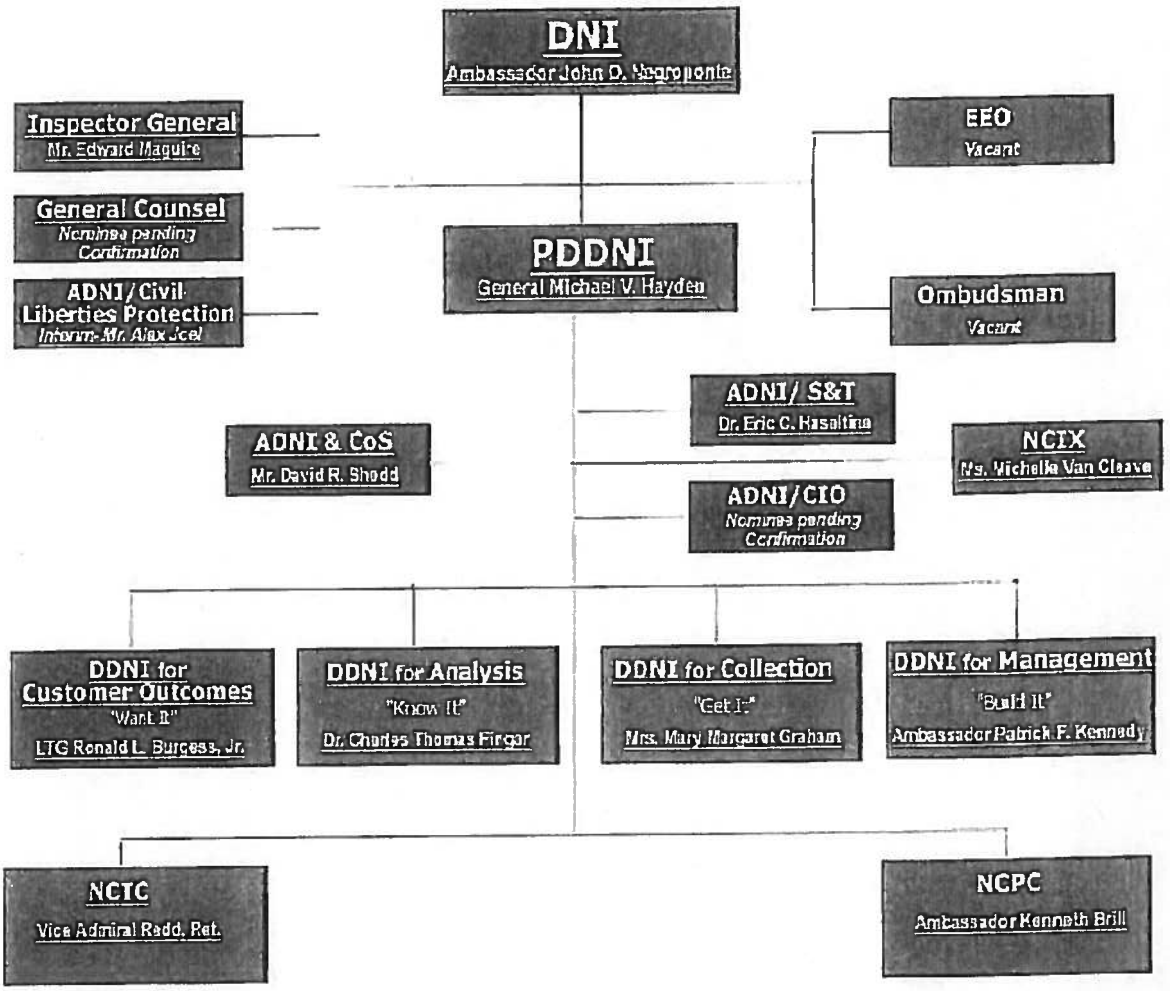
~~(TS//STLW//SI//OC/NF)~~ We found that the ODNI's primary role in the Program was the preparation of 12 ODNI threat assessments approved by the DNI or PDDNI for use in the Program reauthorizations. The ODNI-prepared threat assessments set forth the ODNI's view regarding the existing threat of an al Qaeda terrorist attack against the United States and provided the DNI's recommendation regarding the need to reauthorize the Program. We found that the ODNI threat assessments were drafted by experienced NCTC personnel under the supervision of knowledgeable NCTC supervisors. We noted that the threat assessments were subject to review by OGC and DOJ attorneys before approval. Additionally, we found that the process used by the ODNI to prepare and obtain approval of the threat assessments was straightforward, reasonable, and consistent with the preparation of other documents requiring DNI approval. Overall, we found the ODNI process for the preparation and approval of the threat assessments was responsible and effective.

~~(TS//STLW//SI//OC/NF)~~ We also found that the ODNI oversight components played a limited role in oversight of the Program. The limited ODNI oversight role was due to delays in obtaining Program access for ODNI oversight personnel and to temporary resource limitations related to the stand-up of the agency. However, we believe that the 2008 amendments to EO 12333 and improved staffing levels provide the ODNI oversight components with sufficient resources and authority to fulfill their current oversight responsibilities, assuming timely notification.

This page intentionally left blank.

APPROVED FOR PUBLIC RELEASE

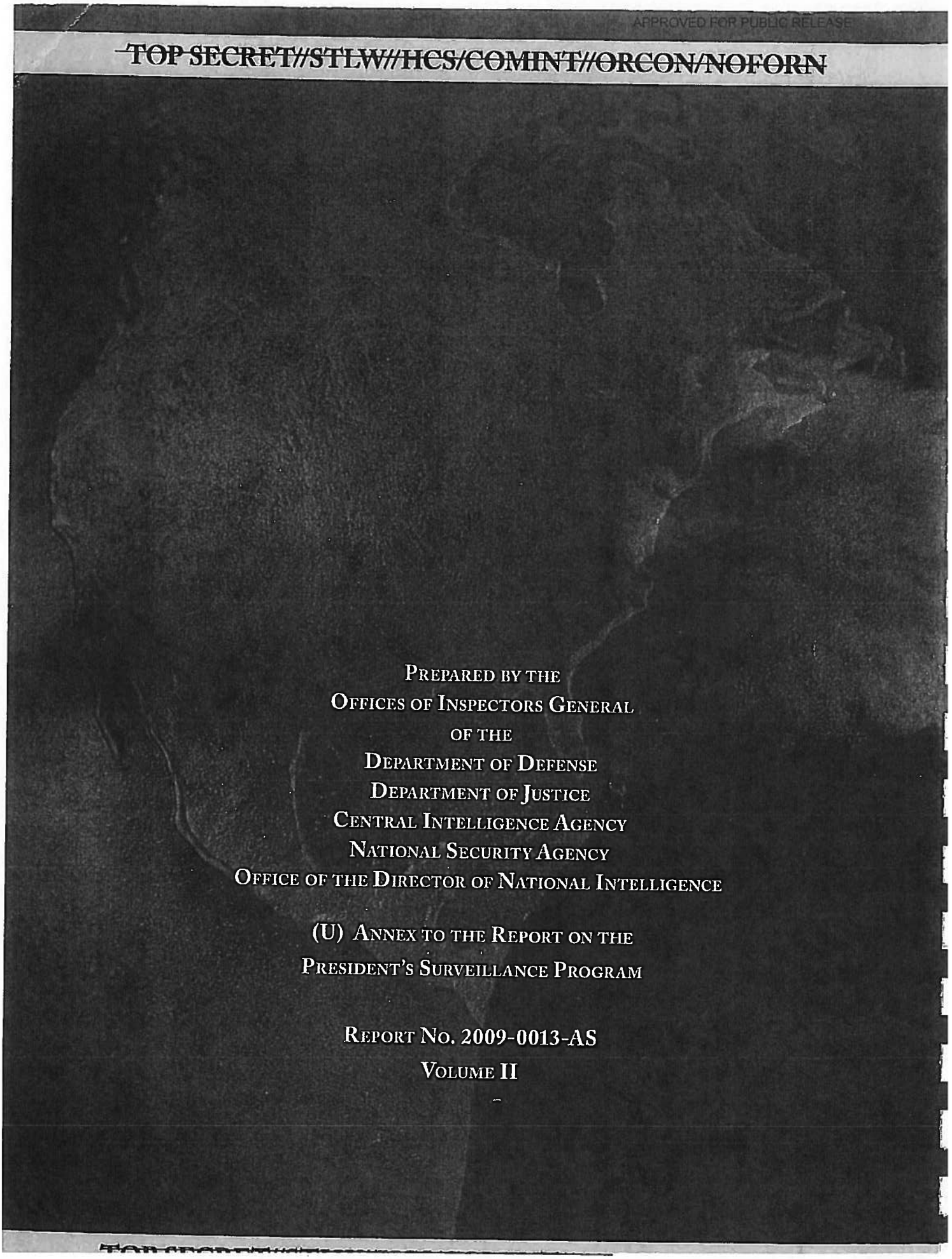
VI. (U) APPENDIX - STRUCTURE OF THE ODNI – 2005



APPROVED FOR PUBLIC RELEASE

APPROVED FOR PUBLIC RELEASE

APPROVED FOR PUBLIC RELEASE



PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

(U) ANNEX TO THE REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

REPORT NO. 2009-0013-AS
VOLUME II

(U) ANNEX TO THE REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

VOLUME III

10 JULY 2009

PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Special Warning

The report contains compartmented, classified material and no secondary distribution may be made without prior consent of the participating Inspectors General. Improper disclosure of this report may result in criminal, civil, or administrative penalties.

REPORT NO. 2009-0013-AS

APPROVED FOR PUBLIC RELEASE

APPROVED FOR PUBLIC RELEASE

U.S. Department of Justice
Office of the Inspector General

A Review of the Department of Justice's Involvement with the President's Surveillance Program (U)

Department of Justice
Office of the Inspector General
Oversight and Review Division
July 2009

~~Derived From: NSA/CSS M 1-52, 2.400~~
~~NSA/CSS M 1-52, 12.48~~
~~Dated: 20070108~~
~~Declassify On: 20340713~~

APPROVED FOR PUBLIC RELEASE

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION (U) 1

I. Methodology of OIG Review (U) 3

II. Organization of this Report (U) 5

CHAPTER TWO: LEGAL AUTHORITIES (U) 7

I. Constitutional, Statutory, and Executive Order Authorities (U) 7

A. Article II, Section 2 of the Constitution (U) 7

B. The Fourth Amendment (U) 7

C. The Foreign Intelligence Surveillance Act (FISA) (U) 8

1. Overview of FISA (U) 8
2. FISA Applications and Orders (U) 10
3. FISA Court (U) 11

D. Authorization for Use of Military Force (U) 12

E. Executive Order 12333 (U) 13

II. Presidential Authorizations (U) 14

A. Types of Collection Authorized ~~(S//NF)~~ 15

B. Findings and Primary Authorities (U) 16

C. The Reauthorization Process (U) 16

D. Approval "as to form and legality" (U) 17

CHAPTER THREE: INCEPTION AND EARLY OPERATION OF STELLAR WIND (SEPTEMBER 2001 THROUGH APRIL 2003) ~~(S//NF)~~ 19

I. Inception of the Stellar Wind Program (U//~~FOUO~~) 19

A. The National Security Agency (U) 19

B. Implementation of the Program (September 2001 through November 2001) ~~(S//NF)~~ 20

1. Pre-Stellar Wind Office of Legal Counsel Legal Memoranda (U) 23
2. Presidential Authorization of October 4, 2001 ~~(TS//SI//NF)~~ 28

C. Presidential Authorization is Revised and the Office of Legal Counsel Issues Legal Memoranda in Support of the Program (November 2001 through January 2002) ~~(TS//STLW//SI//OC/NF)~~ 31

1. Presidential Authorization of November 2, 2001 ~~(TS//SI//NF)~~ 31
2. Yoo Drafts Office of Legal Counsel Memorandum Addressing Legality of Stellar Wind ~~(TS//STLW//SI//OC/NF)~~ 33
3. Additional Presidential Authorizations (U) 38
4. Subsequent Yoo Opinions (U) 39
5. Yoo's Communications with the White House (U) 40
6. Gonzales's View of the Department's Role in Authorizing the Stellar Wind Program ~~(S//NF)~~ 41

II. NSA's Implementation of the Stellar Wind Program (U//~~FOUO~~) 42

A. Implementation of Stellar Wind (U//~~FOUO~~) 42

1. Basket 1 – Telephone and E-Mail Content Collection ~~(TS//STLW//SI//OC/NF)~~ 44
2. Basket 2 – Telephony Meta Data Collection ~~(TS//STLW//SI//OC/NF)~~ 48
3. Basket 3 – E-Mail Meta Data Collection ~~(TS//STLW//SI//OC/NF)~~ 51

B. NSA Process for Analyzing Information Collected Under Stellar Wind ~~(S//NF)~~ 52

1. Basket 1: Content tasking, Analysis, and Dissemination ~~(TS//STLW//SI//OC/NF)~~ 52
2. Baskets 2 and 3: Telephony and E-Mail Meta Data Queries, Analysis, and Dissemination ~~(TS//STLW//SI//OC/NF)~~ 54

III. FBI's Early Participation in the Stellar Wind Program ~~(S//NF)~~ 58

A. FBI Director First Informed of Stellar Wind Program (U//~~FOUO~~) 59

B. [redacted] 59

C. FBI Begins to Receive and Disseminate Stellar Wind "Tippers" ~~(S//NF)~~ 63

1. FBI Initiates [redacted] (S//NF) 63
2. FBI Field Offices' Response to [redacted] Leads ~~(S//NF)~~ 67

3. FBI's Efforts to Track Stellar Wind Tippers and Update Executive Management on Status of [redacted] Leads ~~(S//NF)~~ 69

IV. Justice Department Office of Intelligence Policy and Review's (OIPR) and FISA Court's Early Role in Stellar Wind ~~(TS//STLW//SI//OC/NF)~~ 70

A. Overview of OIPR (U) 71

B. OIPR Counsel Learns of Stellar Wind Program (U//~~FOUO~~) 71

C. FISA Court is Informed of Stellar Wind ~~(TS//SI//NF)~~ 74

D. OIPR Implements "Scrubbing" Procedures for Stellar Wind Information in International Terrorism FISA Applications ~~(TS//STLW//SI//OC/NF)~~ 78

1. Initial Scrubbing Procedures ~~(TS//SI//NF)~~ 79
2. Complications with Scrubbing Procedures ~~(TS//SI//NF)~~ 81

E. Judge Kollar-Kotelly Succeeds Judge Lamberth as FISA Court Presiding Judge (U) 83

1. Judge Kollar-Kotelly Modifies OIPR Scrubbing Procedures ~~(TS//SI//NF)~~ 83
2. OIPR implements Judge Kollar-Kotelly's Scrubbing Procedure ~~(TS//SI//NF)~~ 85

V. FBI Initiates Measures to Improve the Management of Stellar Wind Information ~~(S//NF)~~ 88

A. CAU Acting Unit Chief Evaluates FBI Response to Stellar Wind ~~(S//NF)~~ 89

B. FBI Increases Cooperation with NSA and Initiates [redacted] Project to Manage Stellar Wind Information ~~(TS//STLW//SI//OC/NF)~~ 90

C. FBI Assigns CAU Personnel to NSA on Full-Time Basis ~~(S//NF)~~ 93

VI. OIG Analysis (U) 94

CHAPTER FOUR: LEGAL REASSESSMENT OF STELLAR WIND (MAY 2003 THROUGH MAY 2004) ~~(TS//SI//NF)~~ 99

I. Justice Department Reassesses Legality of Stellar Wind Program ~~(TS//SI//NF)~~ 99

A. Overview of Office of Legal Counsel (U) 99

B. Personnel Changes within Office of Legal Counsel (U) 100

1. Yoo's Role in the Program (October 2001 through May 2003) (U) 100
2. Philbin Replaces Yoo (U) 103
3. Initial Concerns with Yoo's Analysis (U) 104
4. Problems with [redacted] ~~(TS//STLW//SI//OC/NF)~~ 106
5. Other Collection Concerns ~~(S//NF)~~ 108
6. Decision to Draft New OLC Memorandum (U) 108

C. Reassessment of Legal Rationale for the Program ~~(TS//SI//NF)~~ 109

1. Goldsmith Becomes OLC Assistant Attorney General (U) 109
2. NSA Denied Access to OLC Memoranda (U//~~FOUO~~) 111
3. Goldsmith Joins Effort to Reassess Legal Basis for the Program ~~(TS//SI//NF)~~ 112
4. AUMF Becomes the Primary Legal Rationale Supporting [redacted] of the Stellar Wind Program ~~(TS//STLW//SI//OC/NF)~~ 113
5. Office of Legal Counsel Raises its Reassessment of the Stellar Wind Program (December 2003 through January 2004) ~~(TS//SI//NF)~~ 115
6. Deputy Attorney General Comey is Read into the Program (U) 118

D. Office of Legal Counsel Presents its Conclusions to the White House (U) 119

1. March 4, 2004: Comey Meets with Ashcroft to Discuss Problems with the Program (U) 120
2. March 5, 2004: Comey Determines Ashcroft is "Absent or Disabled" (U) 121
3. March 5, 2004: Goldsmith and Philbin Seek Clarification from White House on Presidential Authorizations (U) 122
4. March 6 to 8, 2004: The Department Concludes That Yoo's Legal Memoranda Did Not Cover the Program (U) 124
5. March 9, 2004: White House Seeks to Persuade Department and FBI to Support Continuation of the Program ~~(S//NF)~~ 126
6. Conflict Ensues between Department and White House (U) 129

II. White House Continues Program without Justice Department's Certification ~~(TS//SI//NF)~~ 130

A. White House Counsel Gonzales Certifies March 11, 2004, Presidential Authorization ~~(TS//SI//NF)~~ 131

1. March 10, 2004: Office of Legal Counsel Presses for Solicitor General to be Read into Program (U) 131
2. March 10, 2004: Congressional Leaders Briefed on Situation (U) 131
3. March 10, 2004: Hospital Visit (U) 134
4. March 10, 2004: Olson is Read into the Program (U). 140
5. March 11, 2004: Goldsmith Proposes Compromise Solution (U) 141
6. March 11, 2004: White House Asserts that Comey's Status as Acting Attorney General was Unclear (U) 142
7. March 11, 2004: Gonzales Certifies Presidential Authorization as to Form and Legality ~~(TS//SI//NF)~~ . 144

B. Department and FBI Officials React to Issuance of March 11, 2004, Authorization ~~(TS//SI//NF)~~ 148

1. Initial Responses of Department and FBI Officials (U) 149
2. Department and FBI Officials Consider Resigning (U) 152
3. Comey and Mueller Meet with President Bush (U)..... 155
4. Comey Directs Continued Cooperation with NSA (U) .. 157
5. Department Conducts Additional Legal Analysis (U)... 158
6. Comey Determines that Ashcroft Remains "Absent or Disabled" (U) 163
7. Judge Kollar-Kotelly Briefed on Lack of Attorney General Certification (U) 164
8. Comey and Gonzales Exchange Documents Asserting Conflicting Positions (U) 164

C. White House Agrees to [redacted] ~~(TS//STLW//SI//OC/NF)~~ 168

1. March 19, 2004, Modification (U)..... 168
2. [redacted] 172
3. [redacted] ..173
4. [redacted] 175
5. Judge Kollar-Kotelly is Presented with the OLC Legal Analysis Regarding [redacted] ~~(TS//STLW//SI//OC/NF)~~..... 175
6. April 2, 2004, Modification (U) 178

7. [redacted] Standard is Conveyed to the FBI ~~(TS//SI//NF)~~ 180
8. Office of Legal Counsel Assesses NSA's Compliance with New Collection Standards ~~(TS//SI//NF)~~ 180
9. May 5, 2004, Presidential Authorization ~~(TS//SI//NF)~~ 181
10. May 6, 2004, OLC Memorandum ~~(TS//SI//NF)~~ 182

III. OIG Analysis (U) 186

A. Department's Access to and Legal Review of Stellar Wind Program Through May 2004 ~~(TS//SI//NF)~~ 186

B. The Hospital Visit (U) 197

C. Recertification of the Presidential Authorization and Modification of the Program (U) 199

CHAPTER FIVE: STELLAR WIND PROGRAM'S TRANSITION TO FISA AUTHORITY (JUNE 2004 THROUGH AUGUST 2007) 203

I. E-Mail Meta Data Collection Under FISA ~~(TS//SI//NF)~~ 203

A. Application and FISA Court Order (U) 203

1. Decision to Seek a Pen Register and Trap and Trace (PR/TT) Order from the FISA Court ~~(TS//SI//NF)~~ 203
2. Briefing for Judge Kollar-Kotelly (U) 205
3. The PR/TT Application ~~(TS//SI//NF)~~ 205
4. Judge Kollar-Kotelly Raises Questions about PR/TT Application ~~(TS//SI//NF)~~ 212
5. FISA Court Order (U) 213

B. President Orders Limited Use [redacted] ~~(TS//STLW//SI//OC/NF)~~ 217

1. The President's August 9, 2004, Memorandum to the Secretary of Defense ~~(TS//SI//NF)~~ 217
2. Office of Legal Counsel Determines [redacted] ~~(TS//STLW//SI//OC/NF)~~ 218

C. Non-Compliance with PR/TT Order ~~(TS//SI//NF)~~ 219

1. Filtering Violations ~~(TS//SI//NF)~~ 219
2. FISA Court Renews PR/TT Order ~~(TS//SI//NF)~~ 221
3. [redacted] 222

D. Subsequent PR/TT Applications and Orders ~~(TS//SI//NF)~~ . 224

II. Telephony Meta Data Collection Under FISA ~~(TS//SI//NF)~~ 225

A. Decision to Seek Order Compelling Production of Call detail records ~~(TS//SI//NF)~~ 226

B. Summary of Department's Application and Related FISA Court Order ~~(S/NF)~~ 228

C. Non-Compliance with Section 215 Orders ~~(TS//SI//NF)~~ 232

III. Content Collection under FISA ~~(TS//SI//NF)~~ 237

A. Decision to Seek Content Order ~~(TS//SI//NF)~~ 237

B. Summary of Department's December 13, 2006, Content Application ~~(TS//SI//NF)~~ 239

C. Judge Howard Grants Application in Part ~~(TS//SI//NF)~~ 245

D. Domestic Selectors Application and Order ~~(TS//SI//NF)~~ 248

E. Last Stellar Wind Presidential Authorization Expires ~~(TS//SI//NF)~~ 250

F. First Domestic and Foreign Selectors FISA Renewal Applications ~~(TS//SI//NF)~~ 251

G. Revised Renewal Application for Foreign Selectors and Order ~~(TS//SI//NF)~~ 255

IV. The Protect America Act and the FISA Amendments Act of 2008 (U) 259

A. The Protect America Act (U) 260

B. The FISA Amendments Act of 2008 (U) 264

V. OIG Analysis (U) 267

CHAPTER SIX: [redacted] ~~(S//NF)~~ 271

I. [redacted] Process ~~(S//NF)~~ 272

II. FBI's Decision to Issue National Security Letters under [redacted] to Obtain Telephone Subscriber Information ~~(S//NF)~~ 277

III. [redacted] and Scrubbing Process ~~(TS//SI//NF)~~ 284

IV. Impact of Stellar Wind Information on FBI Counterterrorism Efforts ~~(S//NF)~~ 291

A. Stellar Wind/[redacted] Statistics ~~(TS//STLW//SI//OC/NF)~~ 291

B. FBI Field Office Investigations of [redacted] Tippers ~~(S//NF)~~ 296

C. FBI Statistical Surveys of [redacted] Meta Data Tippers ~~(TS//STLW//SI//OC/NF)~~ 300

1. Early 2006 Survey of [redacted] Telephony and E-Mail Meta Data Tippers ~~(TS//STLW//SI//OC/NF)~~ 301
2. January 2006 Survey of [redacted] E-Mail Meta Data Tippers ~~(TS//STLW//SI//OC/NF)~~ 304

D. FBI Judgmental Assessments of Stellar Wind Information ~~(S//NF)~~ 305

E. Examples of FBI Counterterrorism Cases Involving Stellar Wind Information ~~(S//NF)~~ 310

1. [redacted] 311
2. 313
3. 315
4. 318
5. 322

V. OIG Analysis (U) 325

CHAPTER SEVEN: DISCOVERY ISSUES RELATED TO STELLAR WIND INFORMATION ~~(TS//SI//NF)~~ 333

I. Relevant Law (U) 333

II. Cases Raise Questions about Government's Compliance with Discovery Obligations (U) 335

A. [redacted] 335

B. 336

III. Criminal Division Examines Discovery Issues (U) 340

A. The "Informal Process" for Treating Discovery Issues in International Terrorism Cases (U) 341

B. [redacted] Memorandum Analyzing Discovery Issues Raised by the Stellar Wind Program ~~(TS//STLW//SI//OC/NF)~~ 342

C. Office of Legal Counsel and Discovery Issue (U) 346

IV. Use of the Classified Information Procedures Act (CIPA) to Respond to Discovery Requests (U) 347

A. Overview of CIPA (U) 348

B. Use of CIPA in International Terrorism Prosecutions Alleged to Involve Stellar Wind-Derived Information ~~(TS//STLW//SI//OC/NF)~~ 348

C. Government Arguments in Specific Cases (U) 351

[redacted] 351
..... 353
..... 354
..... 355

V. OIG ANALYSIS (U) 357

CHAPTER EIGHT: PUBLIC STATEMENTS ABOUT THE SURVEILLANCE PROGRAM (U) 361

I. Summary of the Dispute about the Program (U) 361

II. The New York Times Articles and President Bush's Confirmation Regarding NSA Activities (U) 363

III. Other Administration Statements (U) 365

IV. Testimony and Other Statements (U) 366

A. Gonzales's February 6, 2006, Senate Judiciary Committee Testimony (U) 367

B. Comey's May 15, 2007, Senate Judiciary Committee Testimony (U) 370

C. Gonzales's June 5, 2007, Press Conference (U) 371

D. Gonzales's July 24, 2007, Senate Judiciary Committee Testimony (U) 371

E. FBI Director Mueller's July 26, 2007, House Committee on the Judiciary Testimony (U) 376

F. Gonzales's Follow-up Letter to the Senate Judiciary Committee (U) 377

V. OIG Analysis (U) 378

CHAPTER NINE: CONCLUSIONS (U) 387

I. Operation of the Program (U//~~FOUO~~) 388

II. Office of Legal Counsel's Analysis of the Stellar Wind Program ~~(TS//SI//NF)~~ 389

III. Hospital Visit and White House Recertification of the Program (U) 394

IV. Transition of Program to FISA Authority ~~(TS//STLW//SI//OC/NF)~~ 396

V. Impact of Stellar Wind Information on FBI Counterterrorism Efforts ~~(S//NF)~~ 397

VI. Discovery and "Scrubbing" Issues ~~(TS//SI//NF)~~ 402

VII. Gonzales's Statements (U) 404

VIII. Conclusion (U) 406

CHAPTER ONE
INTRODUCTION (U)

On October 4, 2001, three weeks after the terrorist attacks of September 11, 2001, the President issued a Top Secret Presidential Authorization to the Secretary of Defense directing that the signals intelligence capabilities of the National Security Agency (NSA) be used to detect and prevent further attacks in the United States. The Presidential Authorization stated that an extraordinary emergency existed permitting the use of electronic surveillance within the United States for counterterrorism purposes, without a court order, under certain circumstances. For over 6 years, this Presidential Authorization was renewed at approximately 30 to 45 day intervals to authorize the highly classified NSA surveillance program, which was given the cover term "Stellar Wind."[1] ~~(TS//STLW//SI//OC/NF)~~

Under these Presidential Authorizations and subsequently obtained Foreign Intelligence Surveillance Court (FISA Court) orders, the NSA intercepted the content of international telephone and e-mail communications of both U.S. and non-U.S. persons when certain criteria were met. In addition, the NSA collected vast amounts of telephony and e-mail meta data – that is, communications signaling information showing contacts between and among telephone numbers and e-mail addresses, but not including the contents of the communications. [redacted][2] ~~(TS//STLW//SI//OC/NF)~~

Within the Department of Justice (Department or Justice Department) and the Intelligence Community, the different types of information collected under the NSA program came to be referred to as three different "baskets" of information. The collection of the content of telephone and e-mail

---

[1] This program is also known as the President's Surveillance Program (PSP). In Title III of the Foreign Intelligence Surveillance Act Amendments Act of 2008 (FISA Amendments Act), the President's Surveillance Program is defined as

> the intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005 (commonly known as the Terrorist Surveillance Program).

FISA Amendments Act, Title III, Sec. 301(a)(3). (U)

[2] [redacted]

communications was referred to as basket 1. The collection of telephone meta data – including information on the date, time, and duration of the telephone call, the telephone number of the caller, and the number receiving the call – was referred to as basket 2. The collection of e-mail meta data – including the "to," "from," "cc," "bcc," and "sent" lines of an e-mail, but not the "subject" line or content of the e-mail – was referred to as basket 3. ~~(TS//STLW//SI//OC/NF)~~

The content and meta data information was used by the NSA, working with other members of the Intelligence Community, to generate intelligence reports. [redacted] By March 2006, over [redacted] individual U.S. telephone numbers and [redacted] e-mail addresses had been "tipped" to the FBI as leads, the vast majority of which were disseminated to FBI field offices for investigation or other action. Some Stellar Wind-derived information also was disseminated to the larger Intelligence Community through traditional intelligence reporting channels.[3] ~~(TS//STLW//SI//OC/NF)~~

In addition to the FBI's receipt of information from the program, the Justice Department was involved in the program in other ways. Most significantly, the Department's Office of Legal Counsel (OLC) provided advice to the White House and the Attorney General on the overall legality of the Stellar Wind program. In addition, the Department's Office of Intelligence Policy and Review (now called the Office of Intelligence in the Department's National Security Division) worked with the FBI and NSA to justify the inclusion of Stellar Wind-derived information in applications seeking orders under the Foreign Intelligence Surveillance Act (FISA), and when unable to do so, to exclude such information from the applications. The Department's National Security Division (NSD) also submitted classified *ex parte* legal filings in federal courts to address any Stellar Wind reporting concerning defendants during discovery in international terrorism prosecutions. ~~(TS//STLW//SI//OC/NF)~~

Beginning in December 2005, aspects of the Stellar Wind program were publicly disclosed in media reports, originally in a series of articles by The New York Times. After these articles disclosed the telephone and e-mail content collection (basket 1), the President, Attorney General Alberto Gonzales, and other Administration officials publicly confirmed the

[3] The larger Intelligence Community also includes components within other Departments, such as the Departments of Homeland Security, Treasury, Defense, and State. (U)

existence of this part of the program. However, the other aspects of the program – the collection of telephone and e-mail meta data – have not been publicly confirmed. ~~(TS//STLW//SI//OC/NF)~~

The President and other Administration officials labeled the NSA collection of information that was publicly disclosed as "the Terrorist Surveillance Program," although this name was sometimes used within the Intelligence Community to refer to the entire Stellar Wind program. The program was also referred to by other names, such as the "Warrantless Wiretapping Program" or the "NSA Surveillance Program." As discussed above, the technical name for the program, and the term we generally use throughout this report, is the Stellar Wind program.[4] ~~(S//NF)~~

This report describes the Office of the Inspector General's (OIG) review of the Department's role in the Stellar Wind program. Our review discusses the evolution of the Stellar Wind program, including the changes in the Department's legal analyses of the program, the operational changes to the program, and the eventual transition of the program from presidential authority to statutory authority under FISA. The report also assesses the FBI's use of information derived from the Stellar Wind program, including the impact of the information in FBI counterterrorism investigations. ~~(TS//STLW//SI//OC/NF)~~

I. Methodology of OIG Review (U)

During the course of this review, the OIG conducted approximately 80 interviews. Among the individuals we interviewed were former White House Counsel and Attorney General Gonzales; former Deputy Attorney General James Comey; former NSA Director Michael Hayden; FBI Director Robert Mueller, III; former Counsel for Intelligence Policy James Baker; former Assistant Attorneys General for OLC Jay Bybee and Jack Goldsmith; former Principal Deputy and Acting Assistant Attorney General for OLC Steven Bradbury; former Deputy Assistant Attorney General for OLC and Associate Deputy Attorney General Patrick Philbin; and former Assistant Attorneys General for the NSD Kenneth Wainstein and Patrick Rowan. We also interviewed senior FBI Counterterrorism Division officials, the FBI General Counsel and other FBI attorneys, FBI special agents and intelligence analysts, and senior officials in the Department's Criminal and National Security Divisions.[5] (U)

---

[4] Stellar Wind is classified as a Top Secret/Sensitive Compartmented Information program. ~~(S//NF)~~

[5] Although the FBI is a component of the Department of Justice, references in this report to Department officials generally mean non-FBI Department officials. This

(Cont'd.)

We attempted to interview former Attorney General John Ashcroft, but he declined our request for an interview. (U)

In addition, we attempted to interview former Deputy Assistant Attorney General for OLC John Yoo, who drafted the early legal memoranda supporting the legality of the Stellar Wind program. Yoo, through his counsel, declined our request for an interview. ~~(TS//SI//NF)~~

We also attempted to interview White House officials regarding the program, including Andrew Card, former Chief of Staff to President George W. Bush. We made our request for an interview of Card both directly to Card and through the Office of the Counsel to the President (White House Counsel's Office). Card did not grant our request for an interview. Similarly, we attempted to interview David Addington, former Counsel to Vice President Richard B. Cheney. We contacted the Office of the Vice President, but that office did not respond to our request for an interview of Addington. (U)

We believe that we were able to obtain a full picture of the evolution of the program and the theories supporting its legality. However, the refusal by White House officials, former Attorney General Ashcroft, and former Deputy Assistant Attorney General Yoo to be interviewed hampered our ability to fully investigate the process by which the White House and the Justice Department arrived at the initial legal rationale to support the program. In addition, because of our inability to interview Ashcroft, we could not fully determine what efforts the Department took to press the White House for additional Department attorneys to be read into Stellar Wind to work on the legal analysis of the program during its first two years of operation. ~~(TS//SI//NF)~~

In our review, we also examined thousands of electronic and hard copy documents, including the Presidential Authorizations and threat assessments, OLC legal memoranda supporting the program, contemporaneous notes and e-mails of various senior Department and FBI officials, and FISA Court pleadings and orders. We also reviewed NSA materials, including NSA OIG reports on the Stellar Wind program and correspondence between the NSA Office of General Counsel and the Department. ~~(TS//SI//NF)~~

In addition, we received from the FBI an electronic database of its collection of Electronic Communications (EC) that were used to disseminate

---

distinction is especially relevant to our discussion of the number of Department personnel read into the Stellar Wind program, as distinguished from the number of FBI personnel read into the program. (U//~~FOUO~~)

Stellar Wind-derived leads to FBI field offices. This database contained approximately [redacted] ECs, including leads to the FBI's 56 field offices, and responses from those field offices, among other documents. The OIG used this database to confirm information it obtained through interviews and to assist in our analysis of FBI investigations that were based on Stellar Wind information. ~~(TS//STLW//SI//OC/NF)~~

II. Organization of this Report (U)

Chapter Two of this report provides an overview of the primary legal authorities that are relevant to the Stellar Wind program. This chapter also discusses the Presidential Authorizations that were issued to approve the program. (U//~~FOUO~~)

Chapter Three describes the inception and early implementation of the Stellar Wind program from September 2001 through April 2003. This chapter includes a description of the early OLC legal memoranda on the legality of Stellar Wind, how the program was technically implemented, the FBI's early participation in the program, and the FISA Court's first awareness of the program. ~~(TS//SI//NF)~~

Chapter Four covers the period from May 2003 through May 2004 when the legal rationale for the program was substantially reconsidered by the Justice Department. This chapter details in particular the events of March 2004 when the White House decided to continue the program without the Department's certification of a Presidential Authorization. During this time, Attorney General Ashcroft was hospitalized and Deputy Attorney General Comey temporarily exercised the powers of the Attorney General in his capacity as Deputy Attorney General. Comey declined to recertify the Presidential Authorization approving the program based on legal advice he received from OLC Assistant Attorney General Jack Goldsmith, who questioned the adequacy of the legal support for aspects of the program. Comey's decision prompted a significant dispute between the White House and the Justice Department, which resulted in White House Counsel Gonzales and White House Chief of Staff Card visiting Ashcroft in his hospital room in an unsuccessful attempt to have Ashcroft recertify the program. This chapter also describes the background to the dispute, the events related to the hospital visit, the threat by Department officials to resign over the dispute, and the eventual resolution of the dispute. ~~(TS//SI//NF)~~

Chapter Five discusses the transition, in stages, from a program based on Presidential Authorizations to collection activities authorized under the FISA statute. This transition took place in stages between July 2004 and January 2007. This chapter also summarizes legislation in 2007

and 2008 designed to modernize certain provisions of FISA. ~~(TS//STLW//SI//OC/NF)~~

Chapter Six discusses the use of Stellar Wind information by the FBI. It describes the process by which the FBI disseminated Stellar Wind-derived leads to FBI field offices under a program called [redacted] as well as the impact and effectiveness of the Stellar Wind program to the FBI's counterterrorism efforts. ~~(TS//STLW//SI//OC/NF)~~

Chapter Seven examines the Department's handling of discovery issues related to Stellar Wind-derived information in international terrorism prosecutions. ~~(TS//STLW//SI//OC/NF)~~

Chapter Eight analyzes testimony and public statements about aspects of the Stellar Wind program by Attorney General Gonzales. We assess whether the Attorney General's statements, particularly his testimony to the Senate Judiciary Committee in February 2006 and July 2007, were false, inaccurate, or misleading. ~~(S//NF)~~

Chapter Nine contains our conclusions and recommendations. (U)

CHAPTER TWO
LEGAL AUTHORITIES (U)

This chapter summarizes the primary legal authorities referred to throughout this report concerning the Stellar Wind program. These authorities include Article II, Section 2 of the Constitution; the Fourth Amendment to the Constitution; the Foreign Intelligence Surveillance Act; the Authorization for Use of Military Force Joint Resolution (AUMF) passed by Congress after the terrorist attacks of September 11, 2001; Executive Order 12333; and the Presidential Authorizations specifically authorizing the Stellar Wind program. Other authorities, including relevant criminal statutes and judicial opinions, are discussed throughout the report. ~~(TS//SI//NF)~~

I. Constitutional, Statutory, and Executive Order Authorities (U)

A. Article II, Section 2 of the Constitution (U)

Article II, Section 2 of the Constitution, which was one of the primary authorities cited in the Presidential Authorizations in support of the legality of the Stellar Wind program, provides in relevant part:

> The President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service of the United States; he may require the Opinion, in writing, of the principal Officer in each of the executive Departments, upon any Subject relating to the Duties of their respective Offices . . . . ~~(TS//SI//NF)~~

B. The Fourth Amendment (U)

The Fourth Amendment to the Constitution, which also was raised as an important factor in the analysis of the legality of the Stellar Wind program, provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized. ~~(TS//SI//NF)~~

C. The Foreign Intelligence Surveillance Act (FISA)[6] (U)

The Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801, et seq., was enacted in 1978 to "provide legislative authorization and regulation for all electronic surveillance conducted within the United States for foreign intelligence purposes." S. Rep. No. 95-701, at 9 (1978), reprinted in 1978 U.S.C.C.A.N. 3973, 3977. Three major FISA issues are covered in this report. First, as discussed in Chapter Four, FISA was central to a controversy that arose in late 2003 and early 2004 when officials in the Office of Legal Counsel (OLC) and others viewed FISA as potentially in conflict with the legal rationale for at least one aspect of the Stellar Wind program. OLC officials reasoned that if courts viewed FISA in isolation, they might conclude that Congress intended to regulate the President's power to conduct electronic surveillance during wartime, thereby raising questions about the legality of aspects of the program. ~~(TS//STLW//SI//OC/NF)~~

Second, after the FISA Court was informed about the Stellar Wind program in January 2002, it required the government to carefully scrutinize each FISA application to ensure that no Stellar Wind-derived information was relied upon in support of a FISA application without the Court's knowledge, and later without its consent. This process, known as "scrubbing," is discussed in Chapters Three and Six.
~~(TS//STLW//SI//OC/NF)~~

Third, beginning in July 2004, the Stellar Wind program was brought under FISA authority in stages, with the entire program brought under FISA authority by January 2007. In August 2007 and again in July 2008, FISA was amended, and [redacted] The migration of the Stellar Wind program from presidential authority to FISA authority, as well as legislation subsequently enacted to modernize FISA, is discussed in Chapter Five.
~~(TS//STLW//SI//OC/NF)~~

In the following sections, we summarize relevant provisions of FISA as they related to the Stellar Wind program. ~~(TS//SI//NF)~~

1. Overview of FISA (U)

FISA authorizes the federal government to engage in electronic surveillance and physical searches, to use pen register and trap and trace

---

[6] Unless otherwise indicated, all references to FISA are to the statute as it existed prior to the Protect America Act of 2007 and the FISA Amendments Act of 2008. (U)

devices, and to obtain business records to acquire inside the United States foreign intelligence information by, in some instances, targeting foreign powers and agents of foreign powers.[7] FISA also permits the targeting of foreign powers and their agents who are located outside the United States. As a general rule, the FISA Court must first approve an application by the government before the government initiates electronic surveillance. FISA applications must identify or describe the "target" of the surveillance, and must establish probable cause to believe that the target is a "foreign power" or "agent of a foreign power" and that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power."[8] 50 U.S.C. § 1804(a)(4)(A) & (B). ~~(TS//SI//NF)~~

FISA provides four exceptions to the requirement of obtaining judicial approval prior to conducting electronic surveillance: (1) for electronic surveillance directed at certain facilities where the Attorney General certifies that the electronic surveillance is solely directed at communications transmitted by means used exclusively between or among foreign powers or from property under the open and exclusive control of a foreign power, 50 U.S.C. § 1802; (2) where the Attorney General determines an emergency exists and authorizes emergency surveillance until the information sought is obtained, the after-filed application for an order is denied, or the expiration of 72 hours from the time of Attorney General authorization, 50 U.S.C. § 1805(f); (3) for training and testing purposes, 50 U.S.C. § 1805(g); and (4) for 15 days following a congressional declaration of war, 50 U.S.C. § 1811.[9] (U)

The 15-day war declaration exception to FISA's warrant requirement was particularly relevant to the events of 2004, when OLC reassessed its prior opinions concerning the legality of the Stellar Wind program. ~~(TS//SI//NF)~~

---

[7] This report is primarily concerned with the provisions of FISA that authorize electronic surveillance, pen register and trap and trace devices, and access to certain business records. ~~(TS//SI//NF)~~

[8] The terms "foreign power" and "agent of a foreign power" are defined in FISA at 50 U.S.C. § 1801(a) & (b). "Foreign power" is defined, inter alia, as "a group engaged in international terrorism or activities in preparation therefor; . . . ." 50 U.S.C. § 1801(a)(4). An "agent of a foreign power" may be a U.S. person, defined at 50 U.S.C. § 1801(i) to mean, inter alia, a United States citizen or permanent resident alien. The term "facilities" is not defined in FISA. (U)

[9] The Attorney General's emergency surveillance authority under 50 U.S.C. § 1805(f) was extended to 7 days under Section 105(a) of the FISA Amendments Act of 2008. (U)

As discussed in Chapter Four [redacted]

~~(TS//SI//NF)~~

Another FISA provision prohibits persons from intentionally engaging in electronic surveillance "under color of law except as authorized by statute[.]" 50 U.S.C. § 1809(a)(1). As discussed in Chapter Eight, in 2006 the Justice Department asserted in a publicly released legal analysis that this provision did not preclude certain warrantless electronic surveillance activities because such surveillance was "authorized by" subsequent legislative enactments – principally the AUMF. The Department also asserted that the AUMF "confirms and supplements the President's constitutional authority" to conduct warrantless electronic surveillance against the enemy during wartime. (U)

2. FISA Applications and Orders (U)

FISA applications were presented to the FISA Court by the Department's Office of Intelligence Policy and Review (OIPR).[10] Department and FBI officials familiar with the preparation and presentation of FISA applications described this process as extremely time-consuming and labor intensive. (U)

Each application must be approved and signed by the Attorney General (or Acting Attorney General) or Deputy Attorney General and must include the certification of a federal officer identifying or describing the target of the electronic surveillance; a "statement of the facts and circumstances relied upon by the applicant to justify his belief" that the target is a foreign power or agent of a foreign power and that the electronic surveillance is directed at the facilities or places used or to be used by the target; a statement of proposed minimization procedures; and a detailed description of the nature of the information sought and the type of communication or activities to be subjected to the surveillance. 50 U.S.C. § 1804(a)(1)-(6).[11] The application must also include the certification of a

---

[10] The Office of Intelligence Policy and Review became a part of the Department's National Security Division, which was created in September 2006. As of April 2008, the Office of Intelligence Policy and Review was renamed the Office of Intelligence. This organizational change did not affect the FISA application process. (U)

[11] FISA defines minimization procedures as

> [s]pecific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the

(Cont'd.)

high-ranking executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense that the information sought is deemed to be foreign intelligence information, that such information "cannot reasonably be obtained by normal investigative techniques," and that a "significant purpose" of the surveillance is to obtain foreign intelligence information.[12] Id. at § 1804(a)(7). (U)

FISA orders authorize electronic surveillance of U.S. persons for 90 days. FISA orders may be renewed upon the same basis as the underlying order. 50 U.S.C. § 1805(e). As noted, FISA also provides for the emergency use of electronic surveillance. When the Attorney General reasonably determines that an emergency situation exists, the use of electronic surveillance may be approved for a period of up to 72 hours (and under the FISA Amendments Act of 2008, up to 7 days) without a FISA order. 50 U.S.C. § 1805(f). (U)

3. FISA Court (U)

The FISA statute established the FISA Court to review applications and issue orders. The FISA Court initially was composed of seven U.S. District Court judges designated by the Chief Justice of the U.S. Supreme Court to serve staggered, non-renewable 7-year terms.[13] 50 U.S.C.

---

particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information . . . .

50 U.S.C. § 1801(h)(1). (U)

[12] As initially enacted, FISA required officials to certify that "the purpose" of the surveillance was to obtain "foreign intelligence information." However, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the USA PATRIOT Act) was enacted in October 2001 and amended this language in FISA to require only that officials certify that "a significant purpose" of the surveillance was to obtain foreign intelligence information. 50 U.S.C. § 1804(a)(7)(B). This amendment, along with post-September 11 changes to Attorney General guidelines on intelligence sharing procedures and a ruling by the FISA Court of Review, removed the so-called "wall" that had existed between intelligence-gathering activities and criminal investigations. See Memorandum from the Attorney General to Director of the FBI, et al., entitled "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI" (March 6, 2002); *In re Sealed Case*, 310 F.3d 717, 727 (For. Int. Surv. Ct. Rev. 2002)(FISA did not "preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution."). (U)

[13] To achieve staggered terms, the initial appointments ranged from one to seven years. 50 U.S.C. § 1803(d). (U)

§ 1803(a) & (d). The number of judges serving on the FISA Court was increased to 11 by the USA PATRIOT Act of 2001. (U)

D. Authorization for Use of Military Force (U)

On September 18, 2001, in response to the terrorist attacks of September 11, Congress approved an Authorization for Use of Military Force Joint Resolution (AUMF). In conjunction with the President's Commander-in-Chief authority under Article II of the Constitution, this legislation has been cited in support of the President's authority to conduct electronic surveillance without judicial approval. See, e.g., Legal Authorities Supporting the Activities of the National Security Agency Described by the President, January 19, 2006 (Justice Department White Paper), at 6-17. The AUMF states, in pertinent part:

> To authorize the use of the United States Armed Forces against those responsible for the recent attacks launched against the United States.
>
> Whereas, on September 11, 2001, acts of treacherous violence were committed against the United States and its citizens; and
>
> Whereas, such acts render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both at home and abroad; and
>
> Whereas, in light of the threat to the national security and foreign policy of the United States posed by these grave acts of violence; and
>
> Whereas, such acts continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States; and
>
> Whereas, the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States: Now, therefore, be it
>
> Resolved by the Senate and House of Representatives of the United States of America in Congress assembled,
>
> . . .
>
> SEC. 2. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES
>
> (a) IN GENERAL – That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or

persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons. (U)

Pursuant to this authority, the President ordered the U.S. armed forces to invade Afghanistan to combat al Qaeda terrorists and overthrow the Taliban government that had given them refuge. (U)

In 2004, OLC took the position that the AUMF was "expressly designed to authorize whatever military actions the Executive deems appropriate to safeguard the United States[,]" including the use of electronic surveillance to detect and prevent further attacks. See Office of Legal Counsel Memorandum, May 6, 2004, at 31, citing 50 U.S.C. § 1811. In addition, the Justice Department asserted in the 2006 White Paper that in enacting FISA Congress contemplated that a later legislative enactment could authorize electronic surveillance outside the procedures set forth in FISA itself, and cited the AUMF as such a legislative enactment. See Justice Department White Paper at 20-28, citing 50 U.S.C. § 1809(a)(1). ~~(TS//STLW//SI//OC/NF)~~

E. Executive Order 12333 (U)

On December 4, 1981, President Reagan signed Executive Order 12333 as part of a series of legal reforms that followed abuses of intelligence-gathering authority documented by the Church Commission in the 1970s.[14] Executive Order 12333 placed restrictions on intelligence collection activities engaged in by Executive Branch agencies, including the NSA, while also seeking to foster "full and free exchange of information" among these agencies.[15] Executive Order 12333 at 1.1. (U)

Executive Order 12333 provides that the Attorney General is authorized "to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power." Id. at 2.5. Executive Order 12333 also provides that

---

[14] See http://www.aarclibrary.org/publib/church/reports/contents.htm. Volumes 5 and 6 of the Church Commission report address abuses of intelligence-gathering authority by the NSA and the FBI. (U)

[15] Executive Order 12333 was amended on July 30, 2008, by Executive Order 13470. This report refers to Executive Order 12333 as it existed prior to that amendment. (U)

electronic surveillance, as defined under FISA, must be conducted in accordance with FISA.[16] (U)

Executive Order 12333 prohibits the collection of foreign intelligence information by "authorized [agencies] of the Intelligence Community . . . for the purpose of acquiring information concerning the domestic activities of United States persons." Id. at 2.3(b). (U)

However, in authorizing the Stellar Wind program, [redacted] As discussed previously, the legal rationale advanced for this exemption was that the Authorization for Use of Military Force and the President's Commander-in-Chief powers gave the President the authority to collect such information, notwithstanding the FISA statute. ~~(TS//STLW//SI//OC/NF)~~

II. Presidential Authorizations (U)

The Stellar Wind program was first authorized by the President on October 4, 2001, and periodically reauthorized by the President through a series of documents issued to the Secretary of Defense entitled "Presidential Authorization for Specified Electronic Surveillance Activities During a Limited Period to Detect and Prevent Acts of Terrorism Within the United States" (Presidential Authorization or Authorization). A total of 43 Presidential Authorizations, not including modifications and related presidential memoranda, were issued over the duration of the program from October 2001 through February 2007.[17] Each Authorization directed the

---

[16] Prior to September 11, 2001, Executive Order 12333 and FISA were generally viewed as the principal governing authorities for conducting electronic surveillance. For example, in 2000 the NSA reported to Congress that

> (U) The applicable legal standards for the collection, retention, or dissemination of information concerning U.S. persons reflect a careful balancing between the needs of the government for such intelligence and the protection of the rights of U.S. persons, consistent with the reasonableness standard of the Fourth Amendment, as determined by factual circumstances.
>
> (U) In the Foreign Intelligence Surveillance Act (FISA) and Executive Order (E.O.) 12333, Congress and the Executive have codified this balancing. (Citations omitted.)

NSA Report to Congress, *Legal Standards for the Intelligence Community in Conducting Electronic Surveillance* (2000). (U)

[17] The Presidential Authorizations were issued on the following dates: October 4, 2001; November 2, 2001; November 30, 2001; January 9, 2002; March 14, 2002; April 18, 2002; May 22, 2002; June 24, 2002; July 30, 2002; September 10, 2002; October 15, 2002; November 18, 2002; January 8, 2003; February 7, 2003; March 17, 2003; April 22, (Cont'd.)

Secretary of Defense to [redacted] provided the surveillance met certain criteria. The specific criteria are described in detail in Chapters Three and Four of this report. ~~(TS//STLW//SI//OC/NF)~~

A. Types of Collection Authorized ~~(S//NF)~~

The scope of collection permitted under the Presidential Authorizations varied over time, but generally involved intercepting the content of certain telephone calls and e-mails, and the collection of bulk telephone and e-mail meta data. The term "meta data" has been described as "information about information." As used in the Stellar Wind program, for telephone calls, meta data generally refers to "dialing-type information" (the originating and terminating telephone numbers, and the date, time, and duration of the call), but not the content of the call. For e-mails, meta data generally refers to the "to," "from," "cc," "bcc," and "sent" lines of an e-mail, but not the "subject" line or content. ~~(TS//STLW//SI//OC/NF)~~

The information collected through the Stellar Wind program fell into three categories, often referred to as "baskets":

- Basket 1 (content of telephone and e-mail communications);
- Basket 2 (telephony meta data); and
- Basket 3 (e-mail meta data). ~~(TS//STLW//SI//OC/NF)~~

[redacted]

2003; June 11, 2003; July 14, 2003; September 10, 2003; October 15, 2003; December 9, 2003; January 14, 2004; March 11, 2004; May 5, 2004; June 23, 2004; August 9, 2004; September 17, 2004; November 17, 2004; January 11, 2005; March 1, 2005; April 19, 2005; June 14, 2005; July 26, 2005; September 10, 2005; October 26, 2005; December 13, 2005; January 27, 2006; March 21, 2006; May 16, 2006; July 6, 2006; September 6, 2006; October 24, 2006; and December 8, 2006. The last Presidential Authorization expired February 1, 2007. There were also two modifications of a Presidential Authorization and one Presidential memorandum to the Secretary of Defense issued in connection with the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

B. Findings and Primary Authorities (U)

In this section, we describe certain features common to all the Presidential Authorizations. Each of the Presidential Authorizations included a finding to the effect that terrorist groups of global reach possessed the intent and capability to attack the United States, that an extraordinary emergency continued to exist, and that these circumstances "constitute an urgent and compelling governmental interest [redacted] ~~(TS//STLW//SI//OC/NF)~~

The primary authorities cited for the legality of these electronic surveillance and related activities were Article II of the Constitution and the Authorization for Use of Military Force Joint Resolution. [redacted] ~~(TS//STLW//SI//OC/NF)~~ [redacted] The President also noted his intention to inform appropriate members of the Senate and the House of Representatives of the program "as soon as I judge that it can be done consistently with national defense needs." Some Presidential Authorizations described briefings given to members of Congress and FISA Court judges. ~~(TS//STLW//SI//OC/NF)~~

C. The Reauthorization Process (U)

The Presidential Authorizations were issued at intervals of approximately 30 to 45 days. Department officials told the OIG that the intervals were designed to be somewhat flexible to assure the availability of the principals that had to sign the Authorizations and to reassess the reasonableness of the collection.[18] Steven Bradbury, former Principal Deputy and Acting Assistant Attorney General for the Office of Legal Counsel (OLC), said that the main reason for periodically reauthorizing the program was to ensure that the Presidential Authorizations were reviewed frequently to assess the continued need for the program and the program's

[18] The officials who signed the Authorizations included the Attorney General, the President, and the Secretary of Defense (or other high-ranking Department of Defense official). (U//~~FOUO~~)

value. As the period for each Presidential Authorization drew to a close, the Director of Central Intelligence (DCI), and as of June 3, 2005, the Director of National Intelligence (DNI) prepared a threat assessment memorandum for the President describing potential terrorist threats to the United States and outlining intelligence gathered through the Stellar Wind program and other means during the previous Authorization period. The DCI (and later the DNI) and the Secretary of Defense reviewed these memoranda and signed a recommendation that the program be reauthorized.
~~(TS//STLW//SI//OC/NF)~~

Each recommendation was then reviewed by the OLC to assess whether, based on the threat assessment and information gathered from other sources, there was "a sufficient factual basis demonstrating a threat of terrorist attacks in the United States for it to continue to be reasonable under the standards of the Fourth Amendment for the President to [continue] to authorize the warrantless searches involved" in the program. The OLC then advised the Attorney General whether the constitutional standard of reasonableness had been met and whether the Presidential Authorization could be certified "as to form and legality."
~~(TS//STLW//SI//OC/NF)~~

D. Approval "as to form and legality" (U)

As noted above, the Presidential Authorizations were "[a]pproved as to form and legality" by the Attorney General or other senior Department official, typically after the review and concurrence of the OLC. The lone exception to this practice was the March 11, 2004, Authorization which we discuss in Chapter Four. ~~(TS//SI//NF)~~

However, there was no legal requirement that the Authorizations be certified by the Attorney General or other Department official. Former senior Department official Patrick Philbin told us he thought one purpose for the certification was to give the program a sense of legitimacy so that it not "look like a rogue operation." [redacted] Bradbury told us that the Justice Department certifications served as official confirmation that the Department had determined that the activities carried out under the program were lawful.
~~(TS//STLW//SI//OC/NF)~~

Former Attorney General Gonzales told us that certification of the program as to form and legality was not required as a matter of law, but he believed that it "added value" to the Authorization for three reasons. First,

he said that the NSA was being asked to do something it had not done before, and it was important to assure the NSA that the Attorney General had approved the legality of the program. [redacted] Third, for "purely political considerations" the Attorney General's approval of the program would have value "prospectively" in the event of congressional or Inspector General reviews of the program. ~~(TS//STLW//SI//OC/NF)~~

CHAPTER THREE
INCEPTION AND EARLY OPERATION OF STELLAR WIND (SEPTEMBER 2001 THROUGH APRIL 2003) ~~(S//NF)~~

This chapter describes the early operation of the Stellar Wind program. The five sections of the chapter cover the time period from September 2001 to April 2003. ~~(S//NF)~~

In Section I, we provide a brief overview of the National Security Agency (NSA) and the inception of the Stellar Wind program, including a description of the legal authorities relied upon to support the program and the scope of collection authorized under the Presidential Authorizations. In Section II, we describe key aspects of the NSA's implementation of the Presidential Authorizations, [redacted] the technical operation of the program, and the initial process for analyzing and disseminating the information collected. In Sections III and IV, we describe the FBI's and the Office of Intelligence Policy and Review's early knowledge of and involvement in Stellar Wind. In Section V, we describe measures the FBI implemented to improve its management of information derived from the program that the FBI disseminated to its field offices. ~~(TS//STLW//SI//OC/NF)~~

I. Inception of the Stellar Wind Program (U//~~FOUO~~)

A. The National Security Agency (U)

The NSA was established on October 24, 1952, by President Truman as a separate agency within the Department of Defense under the direction, authority, and control of the Secretary of Defense. See Presidential Memorandum to the Secretary of State and the Secretary of Defense, October 24, 1952. By Executive Order 12333 (December 4, 1981), the NSA was given responsibility within the U.S. Intelligence Community for all signals intelligence, including the "collection of signals intelligence for national foreign intelligence purposes" and the processing and dissemination of such intelligence for counterintelligence purposes.[19] (U)

---

[19] Signals intelligence is defined as:

1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. (U)

2. Intelligence derived from communications, electronic, and foreign instrumentation signals. (U)

(Cont'd.)

The NSA's two primary missions are to protect U.S. government information systems and to collect, process, and disseminate foreign signals intelligence information. This twofold mission is reflected in the NSA's organizational structure, which consists of two operational directorates: The Information Assurance Directorate, which conducts defensive information operations to protect information infrastructures critical to the United States' national security interests, and the Signals Intelligence Directorate (SID), which controls foreign intelligence collection and processing activities for the United States. (U)

The SID is divided into three major components, two of which – Analysis and Production [redacted] and Data Acquisition [redacted] – are relevant to the Stellar Wind program. The work of these components with respect to the Stellar Wind program is discussed in more detail in Section II below. ~~(S//NF)~~

B. Implementation of the Program (September 2001 through November 2001) ~~(S//NF)~~

Immediately following the September 11 terrorist attacks, the NSA modified how it conducted some of its traditional signals collection activities. [redacted] ~~(TS//SI//NF)~~

George Tenet, the Director of Central Intelligence at the time, mentioned the modification of these NSA collection activities during a meeting with Vice President Cheney shortly after the September 11 attacks to discuss the intelligence community's response. According to Hayden, who did not attend the meeting but was told about it by Tenet, Cheney asked Tenet to inquire from the NSA whether there were additional steps that could be taken with respect to enhancing signals intelligence capabilities. Tenet related this message to Hayden, who responded that there was nothing further the NSA could do without additional authority. According to Hayden, Tenet asked him a short time later what the NSA could do if additional authority was provided. ~~(TS//SI//NF)~~

Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 484. (U)

Hayden consulted with experts from the NSA's SID and attorneys from the NSA's Office of General Counsel about how the NSA could enhance its collection capabilities consistent with considerations of operational usefulness, technical feasibility, and legality. Hayden said he then attended a meeting at the White House to discuss how NSA signals intelligence collection capabilities could be modified to respond to the September 11 attacks. ~~(TS//SI//NF)~~

Hayden told us he highlighted two issues at this meeting. First, Hayden stated at the meeting that the FISA statute's applicability to evolving telecommunications technology had the effect of constraining the NSA's ability to intercept communications [redacted] According to Hayden, the NSA was authorized under Executive Order 12333 to [redacted] Thus, the NSA could not direct its traditional foreign intelligence collection activities [redacted] without having to first obtain FISA Court authorization.[21] ~~(TS//SI//NF)~~

The second issue Hayden highlighted at the meeting concerned the meta data associated with telephonic and e-mail communications. Hayden said that obtaining access to the meta data of communications to and from

---

[20] The FISA statute defines "wire communication" as "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." 50 U.S.C. § 1801(l). By its terms, FISA governs the acquisition of wire communications to or from persons in the United States if such acquisition occurs in the United States. See 50 U.S.C. § 1801(f)(2). [redacted] (U)

[21] [redacted]

the United States, as well as communications within the United States, would significantly enhance the NSA's analytical capabilities. ~~(TS//SI//NF)~~

Hayden said he attended two additional meetings with Vice President Cheney to discuss further how NSA collection capabilities could be expanded along the lines described at the White House meeting. Vice President Cheney directed Hayden to meet with the Counsel to the Vice President, David Addington, to continue the discussion, which Hayden said he did. According to Hayden, Addington drafted the first Presidential Authorization for the Stellar Wind program based on these meetings.[22] ~~(TS//STLW//SI//OC/NF)~~

The Stellar Wind program officially came into existence on October 4, 2001, when President Bush signed the Presidential Authorization drafted by Addington. The Authorization directed the Secretary of Defense to employ the signals intelligence capabilities of the NSA to collect certain foreign intelligence by electronic surveillance in order to prevent acts of terrorism within the United States.[23] The Presidential Authorization stated that an extraordinary emergency existed because of the September 11 attacks, constituting an urgent and compelling governmental interest permitting electronic surveillance within the United States for counterterrorism purposes without judicial warrants or court orders. ~~(TS//STLW//SI//OC/NF)~~

Access to the Stellar Wind program was very tightly restricted. Former White House Counsel and Attorney General Alberto Gonzales told the OIG that it was the President's decision to keep the program a "close hold." Gonzales stated that the President made the decision on all requests to read in non-operational persons, including Justice Department officials, and that as far as he was aware this decision-making authority had not been delegated either within the White House or to other agencies concerning read-in decisions for operational personnel, such as NSA and

---

[22] Hayden told us he could not recall the Justice Department having any involvement in or presence at meetings he attended to discuss enhancing NSA collection capabilities. Hayden said this mildly surprised him but that he assumed someone was keeping the Department briefed on these discussions. Gonzales, who was the White House Counsel at the time, also told the OIG that he would be "shocked" if the Department was not represented at the White House meetings, and further stated that in the immediate aftermath of September 11, he met often with lawyers from the NSA, CIA, DOD, and the Justice Department with the objective of "coordinating the legal thinking" concerning the United States' response to the attacks. Because we were unable to interview Addington, former Attorney General Ashcroft, and John Yoo, we do not know what role if any the Department played in drafting or reviewing the first Presidential Authorization. ~~(TS//SI//NF)~~

[23] The program was given the cover term [redacted] at which time the cover term was changed to "Stellar Wind." ~~(S//NF)~~

FBI employees.[24] However, as indicated in the NSA Office of the Inspector General's report on the President's Surveillance Program (NSA OIG Report), decisions to read in NSA, CIA, and FBI operational personnel were made by the NSA. According to the NSA OIG Report, NSA Director Hayden needed White House approval to read in members of Congress, FISA Court judges, the NSA Inspector General, and others. See NSA OIG Report at V. ~~(S//NF)~~

1. Pre-Stellar Wind Office of Legal Counsel Legal Memoranda (U)

In this section, we summarize the initial legal memoranda from the Justice Department supporting the legal basis for the Stellar Wind program, and we describe the key aspects of the first Presidential Authorization for the program. ~~(TS//STLW//SI//OC/NF)~~

a. Hiring of John Yoo (U)

OLC Deputy Assistant Attorney General John Yoo was responsible for drafting the first series of legal memoranda supporting the program.[25] As noted above, Yoo was the only OLC official "read into" the Stellar Wind program from the program's inception until he left the Department in May 2003.[26] The only other non-FBI Department officials read into the program until after Yoo's departure were Attorney General Ashcroft, who was read in on October 4, 2001, and Counsel for Intelligence Policy James Baker, who was read in on January 11, 2002.[27] ~~(TS//STLW//SI//OC/NF)~~

---

[24] Gonzales testified before the Senate Judiciary Committee on July 18, 2006, that "[a]s with all decisions that are non-operational in terms of who has access to the program, the President of the United States makes the decisions, because this is such an important program[.]" (U)

[25] The Office of Legal Counsel typically drafts memoranda for the Attorney General and the Counsel to the President, usually on matters involving significant legal issues or constitutional questions, and in response to legal questions raised by Executive Branch agencies. In addition, all Executive Orders proposed to be issued by the President are reviewed by the Office of Legal Counsel as to form and legality, as are other matters that require the President's formal approval. (U)

[26] The process of being "read into" a compartmented program generally entails being approved for access to particularly sensitive and restricted information about a classified program, receiving a briefing about the program, and formally acknowledging the briefing, usually by signing a nondisclosure agreement describing restrictions on the handling and use of information concerning the program. (U)

[27] Daniel Levin, who served as both Chief of Staff to FBI Director Robert Mueller and briefly as Ashcroft's national security counselor, also was read into the program along with Mueller in late September 2001 at the FBI. According to Levin, White House Counsel Gonzales controlled who was read into the program, but Gonzales told him that the President had to personally approve each request. ~~(TS//STLW//SI//OC/NF)~~

Jay Bybee, the Assistant Attorney General for the Office of Legal Counsel from November 2001 through March 2003, provided the OIG with background information on how Yoo came to be involved in national security issues on behalf of the OLC. Bybee's nomination to be the OLC Assistant Attorney General was announced by the White House in July 2001. Bybee was not confirmed by the Senate as the Assistant Attorney General until late October 2001.[28] For several weeks after the September 11, 2001, terrorist attacks, Bybee remained a law professor at the University of Nevada-Las Vegas, and was sworn in as OLC Assistant Attorney General in late November 2001. ~~(TS//SI//NF)~~

Bybee told us that he traveled to Washington, D.C., sometime in July 2001 to interview applicants for Deputy Assistant Attorney General slots in OLC. In early July 2001, Kyle Sampson, at the time a Special Assistant to the President and Associate Director for Presidential Personnel assigned to handle presidential appointments to the Department of Justice, told Bybee that John Yoo was already under consideration for one of the OLC Deputy Assistant Attorney General slots. Bybee said Sampson asked him whether he would agree to have Yoo be one of his deputies. Bybee said that he knew Yoo only by reputation but was "enthusiastic" about the prospect of having Yoo as a Deputy. Bybee told the OIG that he regarded Yoo as a "distinguished hire." Bybee said that after speaking with Sampson he called Yoo and asked him to work at OLC as a Deputy Assistant Attorney General. (U)

In addition to speaking with Yoo, Bybee interviewed other prospective OLC Deputies, and hired several individuals, including Patrick Philbin and Ed Whelan, for those positions.[29] The White House recommended, and Bybee agreed, that Whelan be designated Principal Deputy. Bybee stated that he knew Yoo would be disappointed because Yoo had wanted that position, and Bybee said that Yoo "didn't hide his disappointment." Bybee told us that Yoo asked him whether since he was not selected for the Principal Deputy slot he could be guaranteed the "national security portfolio." Bybee agreed to Yoo's request. Bybee told the OIG that this was an easy decision because Yoo had more national security experience than any of the other deputies. (U)

---

[28] Bybee told us that Daniel Koffsky was the Acting Assistant Attorney General at this time. (U)

[29] Bybee told us that all Deputy candidates were also interviewed by the White House. As described in Chapter Four of this report, Philbin played a central role in the Department's reassessment of the legal basis for the Stellar Wind program after John Yoo left the Department in May 2003. ~~(TS//SI//NF)~~

Bybee said that Yoo began working in OLC in July 2001 and that all of the Deputies were in place before Bybee began serving as head of the OLC that November. (U)

Bybee told us he was never read into the Stellar Wind program and could shed no further light on how Yoo came to draft the OLC opinions on the program. However, he said that Yoo had responsibility for supervising the drafting of opinions related to national security issues by the time the attacks of September 11 occurred.[30] Bybee described Yoo as "articulate and brilliant," and also said he had a "golden resume" and was "very well connected" with officials in the White House. He said that from these connections, in addition to Yoo's scholarship in the area of executive authority during wartime, it was not surprising that Yoo "became the White House's guy" on national security matters. (U)

b. Yoo's Legal Analysis of a Warrantless Domestic Electronic Surveillance Program ~~(TS//SI//NF)~~

Before the start of the Stellar Wind program under the October 4, 2001, Presidential Authorization, Yoo drafted a memorandum evaluating the legality of a "hypothetical" electronic surveillance program within the United States to monitor communications of potential terrorists. His memorandum, dated September 17, 2001, was addressed to Timothy Flanigan, Deputy White House Counsel, and was entitled "Constitutional Standards on Random Electronic Surveillance for Counter-Terrorism Purposes." ~~(TS//STLW//SI//OC/NF)~~

Yoo drafted a more extensive version of this memorandum, dated October 4, 2001, for White House Counsel Gonzales. [redacted] ~~(TS//SI//NF)~~

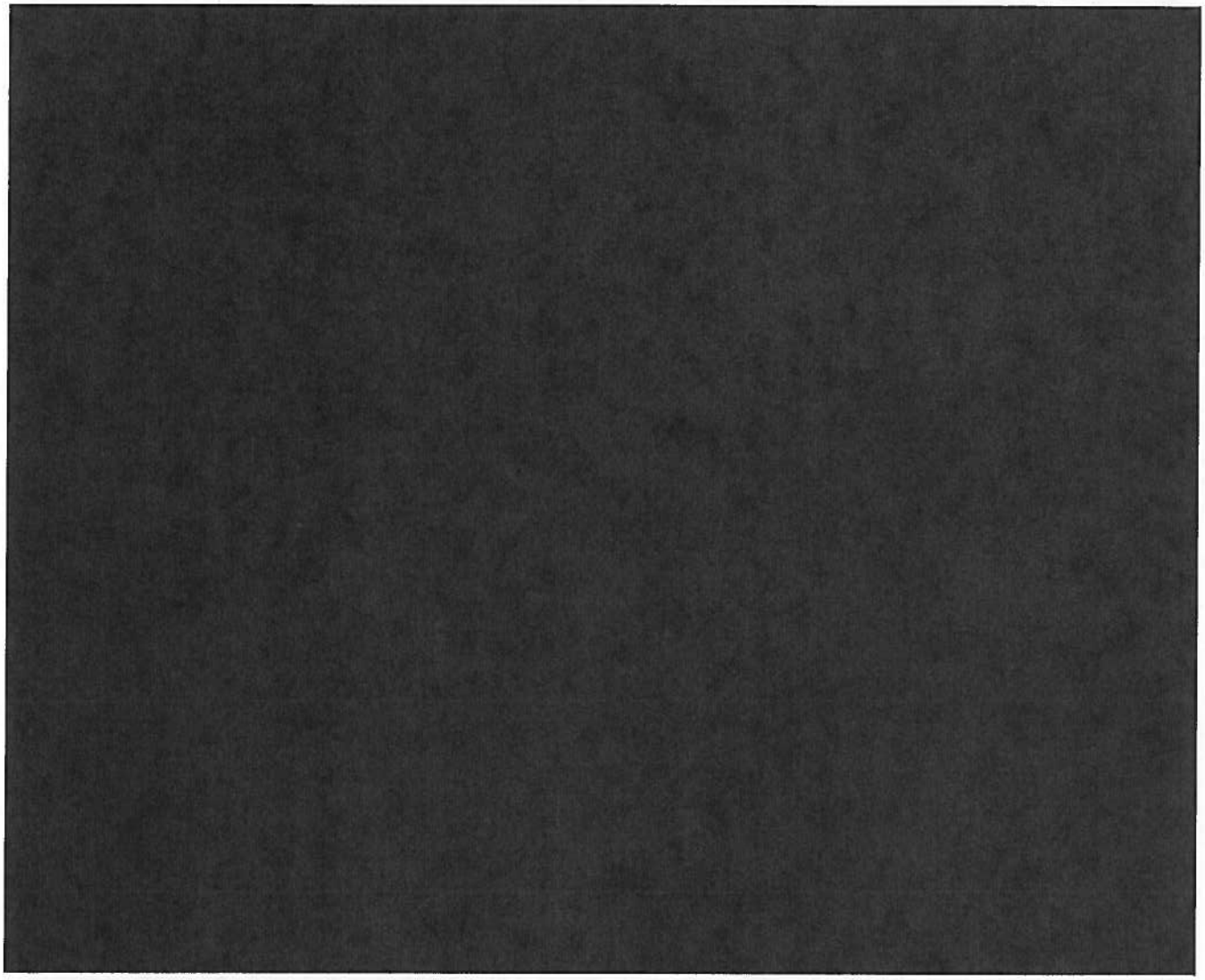
[30] As noted above, Yoo, Ashcroft, Card, and Addington declined or did not respond to our request for interviews, and we do not know how Yoo came to deal directly with the White House on legal issues surrounding the Stellar Wind program. In his book "War by Other Means," Yoo wrote that "[a]s a deputy to the assistant attorney general in charge of the office, I was a Bush Administration appointee who shared its general constitutional philosophy. . . . I had been hired specifically to supervise OLC's work on [foreign affairs and national security]." John Yoo, *War by Other Means*, (Atlantic Monthly Press, 2006), 19-20. ~~(TS//SI//NF)~~

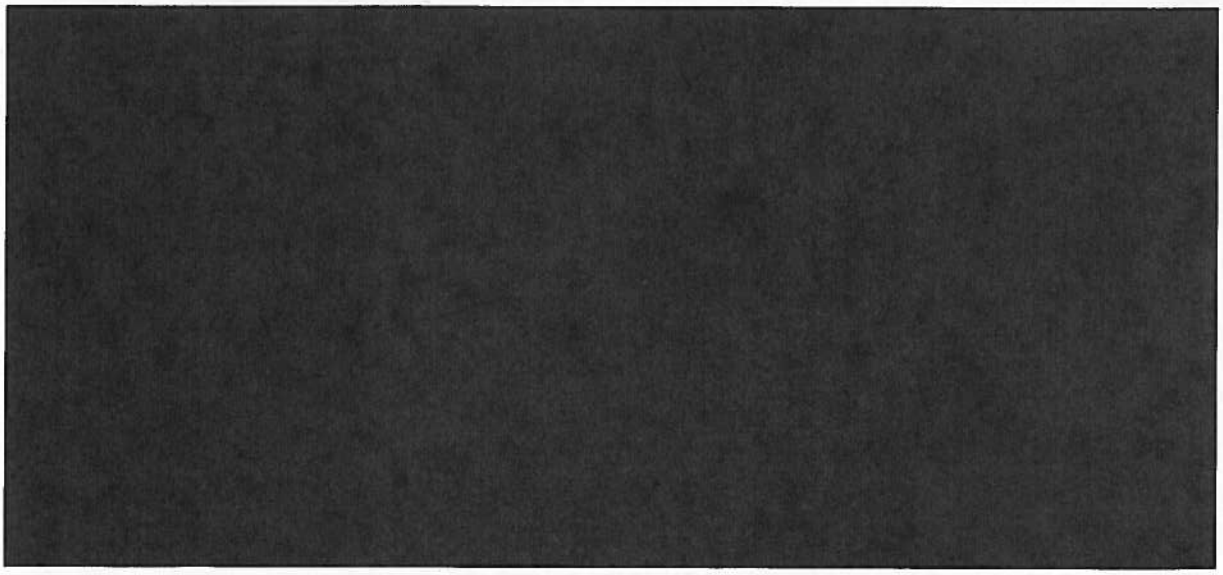
[redacted]

[31] As discussed below, however, his description of how communications would be collected and used under the program differed in key respects from the actual operation of the Stellar Wind program. In fact, in a January 23, 2006, address to the National Press Club, former NSA Director Hayden stated: ~~(TS//SI//NF)~~

> Let me talk for a few minutes also about what this program is not. It is not a drift net over Dearborn or Lackawanna or Freemont grabbing conversations that we then sort out by these alleged keyword searches or data-mining tools or other devices that so-called experts keep talking about. (U)

[redacted]





Yoo's September 17 and October 4 memoranda were not addressed specifically to the Stellar Wind program, but rather to a "hypothetical" randomized or broadly scoped domestic warrantless surveillance program. As discussed below, the first Office of Legal Counsel opinion explicitly addressing the legality of the Stellar Wind program was not drafted until after the program had been formally authorized by President Bush on October 4, 2001. ~~(TS//SI//OC/NF)~~

Gonzales told the OIG that he did not believe these first two memoranda fully addressed the White House's understanding of the Stellar Wind program. Rather, as described above, these memoranda addressed the legality of a "hypothetical" domestic surveillance program rather than the Stellar Wind program as authorized by the President and carried out by the NSA.[35] However, Gonzales also told us that he believed these first two memoranda described as lawful activities that were broader than those carried out under Stellar Wind, and that therefore these opinions "covered" the Stellar Wind program. ~~(TS//SI//NF)~~

2. Presidential Authorization of October 4, 2001 ~~(TS//SI//NF)~~

On October 4, 2001, President Bush issued the first of 43 Presidential Authorizations for the Stellar Wind program. The October 4 Authorization

[redacted]

[35] Gonzales noted that Deputy White House Counsel Timothy Flanigan, the recipient of the first Yoo memorandum, was not read into Stellar Wind. (U//~~FOUO~~)

In short, this first Authorization allowed NSA to intercept the content of any communication, including those to, from, or exclusively within the United States, where probable cause existed to believe one of the communicants was engaged in international terrorism, [redacted] The Authorization also allowed the NSA to "acquire" telephony and e-mail meta data where one end of the communication was foreign or neither communicant was known to be a U.S. citizen.[36] ~~(TS//STLW//SI//OC/NF)~~

The Authorization stated that it relied primarily on Article II of the Constitution and on the recently passed Authorization for the Use of Military Force (AUMF) to support the intelligence-gathering activities. The Authorization also stated that the President's directive was based on threat assessments indicating that terrorist groups remained determined to attack in the United States. The Authorization stated that it was to terminate [redacted] from the date of its execution.
~~(TS//STLW//SI//OC/NF)~~

As several Office of Legal Counsel and other Department and NSA officials acknowledged, in addition to allowing the interception of the content of communications into or out of the United States, the literal terms of paragraph 4(a)(ii) of this first Authorization would have allowed NSA to intercept the content of purely domestic communications. NSA Director Hayden told us he did not realize this until Addington specifically raised the subject during a meeting the two had to discuss renewing the first Authorization. According to Hayden, he told Addington that he did not want the NSA conducting such domestic interceptions and cited three reasons for this. First, he said the NSA was a *foreign* intelligence agency. Second, the NSA's collection infrastructure would not support the collection of purely domestic communications. Third, Hayden said he would require such a high evidentiary standard to justify intercepting purely domestic communication that such cases might just as well go to the FISA Court.[37]
~~(TS//STLW//SI//OC/NF)~~

---

36 [redacted]

37 Hayden said Addington did not pressure him on the subject and simply modified the next Authorization to provide that the NSA may only intercept the content of communications that originated or terminated in the United States. We discuss the modifications to the Authorization in the next part of this chapter.
~~(TS//STLW//SI//OC/NF)~~

As a result, Hayden said the NSA did not exercise the apparent authority in the first Authorization to intercept domestic-to-domestic communications. Goldsmith stated that Hayden's position that the NSA not involve itself in domestic spying related back to NSA's "getting in a lot of trouble" for its abuses during the 1970s. In addition, former Deputy Attorney General Comey told us that Hayden had said he was willing to "walk up to the line" but would be careful "not to get chalk on [his] shoes." ~~(TS//STLW//SI//OC/NF)~~

As discussed above, subsection (b) of paragraph 4 of the Authorization covered the acquisition of both e-mail and telephony meta data. The e-mail meta data included the "to," "from," "cc," "bcc," and "sent" lines of an e-mail, but not the "subject" line or content of the e-mail. [redacted] Telephony meta data acquisition included the dialing information from telephone billing data, such as the originating and terminating telephone number and the date, time, and duration of the telephone calls, but not the content of telephone calls. Under the Presidential Authorization, collection of both e-mail and telephony meta data was limited to circumstances in which one party to the communication was outside the United States or no party to the communication was known to be a U.S. citizen. ~~(TS//STLW//SI//OC/NF)~~

Attorney General Ashcroft approved the first Presidential Authorization as to "form and legality" on October 4, 2001. According to NSA records, this was the same day that Ashcroft was verbally read into the Stellar Wind program. Daniel Levin, who in October 2001 was both a national security counselor to Attorney General Ashcroft and FBI Director Mueller's Chief of Staff, told us that, according to Ashcroft, the Presidential Authorization was "pushed in front of" Ashcroft and he was told to sign it.[38] Levin stated that he was not with Ashcroft when this occurred and therefore he did not have an opportunity to advise Ashcroft about the Authorization before Ashcroft signed it. ~~(TS//STLW//SI//OC/NF)~~

James Baker, Counsel for Intelligence Policy, told us that Levin had given him the same account of how Ashcroft came to approve the October 4, 2001, Presidential Authorization. According to Baker, Ashcroft was told that the program was "critically important" and that it must be approved as to form and legality. Baker said that Levin told him Ashcroft approved the

---

[38] According to Hayden, Addington typed the Presidential Authorizations and personally couriered them around for signatures. However, the OIG was unable to determine whether Addington presented the first Authorization to Ashcroft for signature, because both Ashcroft and Addington declined or did not respond to our requests to interview them. ~~(S//NF)~~

Authorization on the spot. According to Baker, Levin also told Baker that when he learned there was no memorandum from the Office of Legal Counsel concerning the program, Levin told Yoo to draft one. ~~(TS//STLW//SI//OC/NF)~~

Levin's account to us of the instruction that Yoo draft a memorandum concerning the legality of the program differed slightly from Baker's account. Levin told us that he said to Ashcroft that it "wasn't fair" that Ashcroft was the only Justice official read into the program, and that for Ashcroft's protection Levin advised Ashcroft to have another Department official read into the program for the purpose of providing advice on the legality of the program. Levin said he learned that Ashcroft was able to get permission from the White House to have one other person read into the program to advise Ashcroft, although Levin was not certain how Yoo came to be selected as that person.[39] As discussed below, Gonzales told us that it was the President's decision to read John Yoo into the program. ~~(TS//STLW//SI//OC/NF)~~

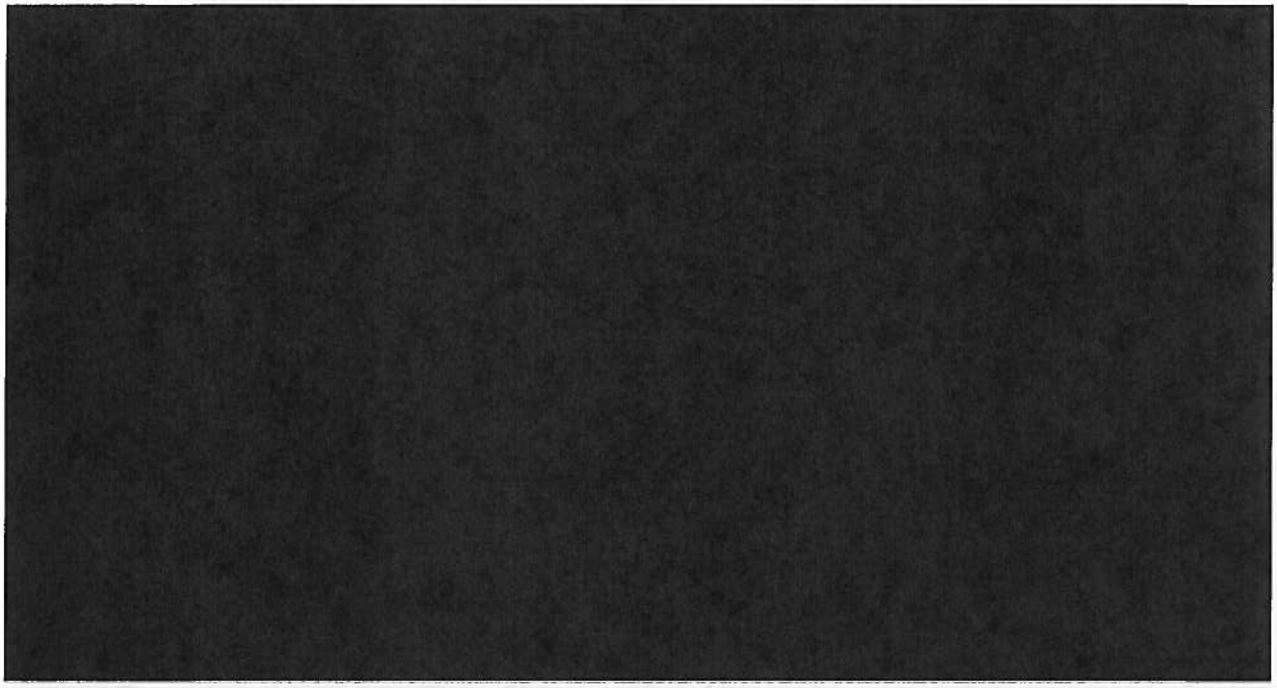
C. Presidential Authorization is Revised and the Office of Legal Counsel Issues Legal Memoranda in Support of the Program (November 2001 through January 2002) ~~(TS//STLW//SI//OC/NF)~~

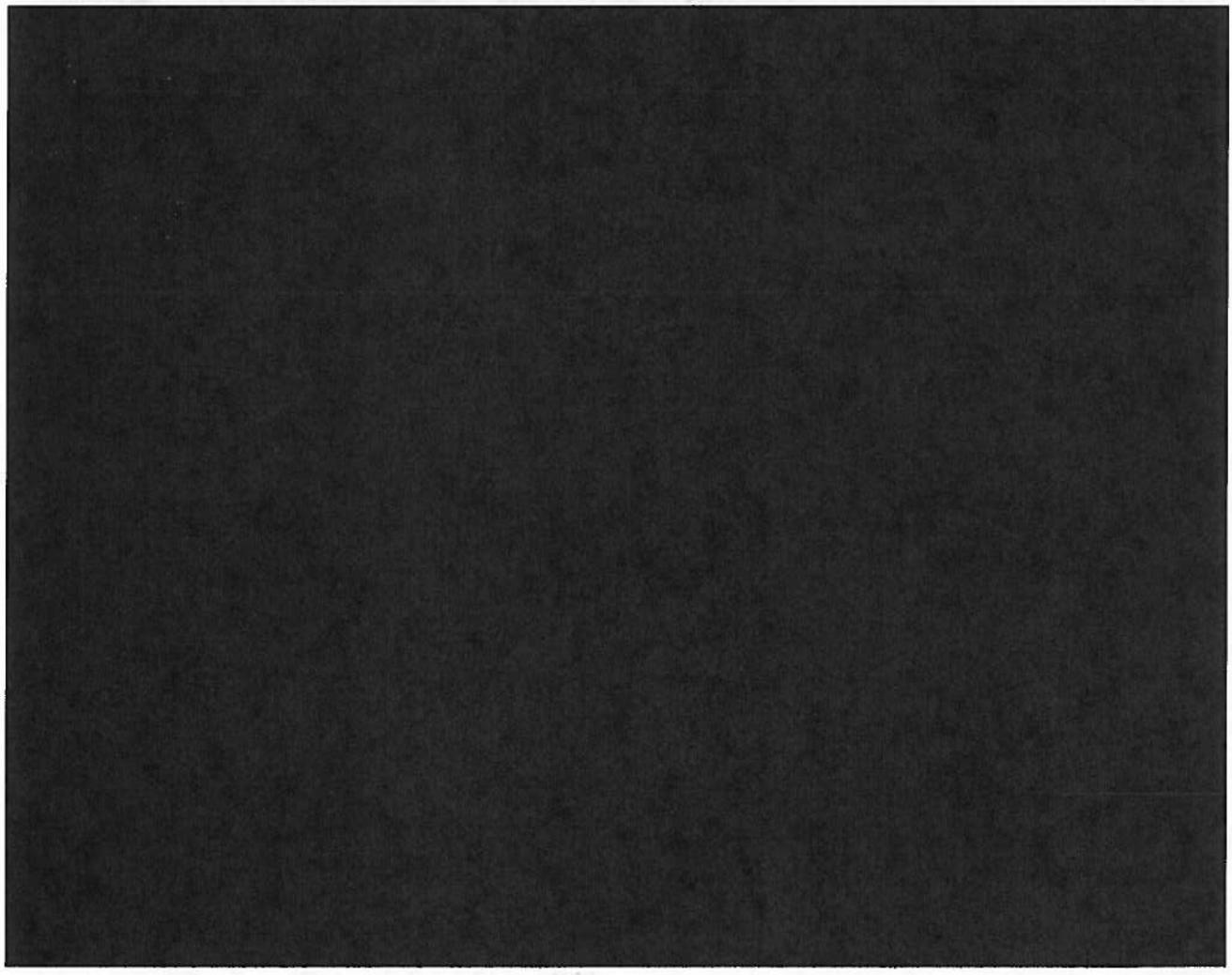
1. Presidential Authorization of November 2, 2001 ~~(TS//SI//NF)~~

On November 2, 2001, with the first Presidential Authorization set to expire, President Bush signed a second Presidential Authorization. The second Authorization relied upon the same authorities in support of the President's actions, chiefly the Article II Commander-in-Chief powers and the AUMF. The second Authorization cited the same findings in a threat assessment as to the magnitude of the potential threats and the likelihood of their occurrence in the future. [redacted]

[redacted]

[39] By October 4, 2001, Yoo had already drafted two legal analyses on a hypothetical warrantless surveillance program and therefore already had done some work related to the program prior to October 4 when Ashcroft was read in. ~~(TS//SI//NF)~~





In addition, former OLC Principal Deputy and Acting Assistant Attorney General Steven Bradbury described this [redacted] ~~(TS//STLW//SI//OC/NF)~~

2. Yoo Drafts Office of Legal Counsel Memorandum Addressing Legality of Stellar Wind ~~(TS//STLW//SI//OC/NF)~~

The Stellar Wind program was first authorized by President Bush and certified as to form and legality by Attorney General Ashcroft on October 4, 2001, without the support of any formal legal opinion from the Office of Legal Counsel expressly addressing Stellar Wind. ~~(TS//SI//NF)~~

The first OLC opinion directly supporting the legality of the Stellar Wind program was dated November 2, 2001, and was drafted by Yoo. His opinion also analyzed the legality of the first Presidential Authorization and a draft version of the second Authorization.[40] ~~(TS//SI//NF)~~

In his November 2 memorandum to Attorney General Ashcroft, Yoo opined that the Stellar Wind program [redacted] As discussed in Chapter Four of this report, however, perceived deficiencies in Yoo's memorandum later became critical to the Office of Legal Counsel's decision to reassess the Stellar Wind program in 2003. We therefore describe Yoo's legal analysis in his November 2 memorandum. ~~(TS//SI//NF)~~

Yoo acknowledged at the outset of his November 2 memorandum that "[b]ecause of the highly sensitive nature of this subject and the time pressures involved, this memorandum has not undergone the usual editing and review process for opinions that issue from our Office [OLC]." The memorandum then reviewed the changes to NSA's collection authority between the first and second Presidential Authorizations. [redacted]

[40] The second Authorization was issued on November 2, 2001. In developing his legal memorandum, Yoo analyzed a draft of the second Authorization dated October 31, 2001. The OIG was not provided the October 31 draft Presidential Authorization, but based on Yoo's description in his November 2 memorandum, it appears that the draft that Yoo analyzed tracked the language of the final November 2, 2001, Authorization signed by the President. ~~(TS//SI//NF)~~

[redacted]

~~(TS//STLW//SI//OC/NF)~~

[redacted]

Yoo did acknowledge in his memorandum that the first Presidential Authorization was "in tension with FISA." Yoo stated that FISA "purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence," but Yoo then opined that "[s]uch a reading of FISA would be an unconstitutional infringement on the President's Article II authorities."[41] Citing advice of the OLC and the position of the Department as presented to Congress during passage of the USA PATRIOT Act several weeks earlier, Yoo characterized FISA as merely providing a "safe harbor for electronic surveillance," adding that it "cannot restrict the President's ability to engage in warrantless searches that protect the national security." ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[41] As discussed in Chapter Four, Goldsmith criticized this statement as conclusory and unsupported by any separation of powers analysis. (U//~~FOUO~~)

Regarding whether the activities conducted under the Stellar Wind program could be conducted under FISA, Yoo wrote that it was problematic that FISA required an application to the FISA Court to describe the [redacted] or "facilities" to be used by the target of the surveillance. Yoo also stated that it was unlikely that a FISA Court would grant a warrant to cover [redacted] as contemplated in the Presidential Authorization. Noting that the Authorization could be viewed as a violation of FISA's civil and criminal sanctions in 50 U.S.C. §§ 1809-10, Yoo opined that in this regard FISA represented an unconstitutional infringement on the President's Article II powers. According to Yoo, the ultimate test of whether the government may engage in warrantless electronic surveillance activities is whether such conduct is consistent with the Fourth Amendment, not whether it meets the standards of FISA. ~~(TS//STLW//SI//OC/NF)~~

Citing cases applying the doctrine of constitutional avoidance, Yoo reasoned that reading FISA to restrict the President's inherent authority to conduct foreign intelligence surveillance would raise grave constitutional questions.[42] Yoo wrote that "unless Congress made a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless searches in the national security area – which it has not – then the statute must be construed to avoid such a reading."[43] ~~(TS//STLW//SI//OC/NF)~~

---

[42] Yoo's memorandum cited the doctrine of constitutional avoidance, which holds that "where an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress." *Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Construction Trades Council*, 485 U.S. 568, 575 (1988). Yoo cited cases supporting the application of this doctrine in a manner that preserves the President's "inherent constitutional power, so as to avoid potential constitutional problems." See, e.g., *Public Citizen v, Department of Justice*, 491 U.S. 440, 466 (1989). ~~(TS//STLW//SI//OC/NF)~~

[43] On March 2, 2009, the Justice Department released nine opinions written by the OLC from 2001 through 2003 regarding "the allocation of authorities between the President and Congress in matters of war and national security" containing certain propositions that no longer reflect the views of the OLC and "should not be treated as authoritative for any purpose." Steven G. Bradbury, Principal Deputy Assistant Attorney General, Office of Legal Counsel, Department of Justice, Memorandum for the Files, "Re: Status of Certain OLC Opinions Issued in the Aftermath of the Terrorist Attacks of September 11, 2001," January 15, 2009, 1, 11. Among these opinions was a February 2002 classified memorandum written by Yoo which asserted that Congress had not included a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless surveillance activities in the national security area and that the FISA statute therefore does not apply to the president's exercise of his Commander-in-Chief authority. In a January 15, 2009, memorandum (included among those released in March), Bradbury stated that this proposition "is problematic and questionable, given FISA's express references to the President's authority" and is "not supported by convincing reasoning." ~~(TS/STLW//SI//OC/NF)~~

Yoo's analysis of this point would later raise serious concerns for other officials in the Office of Legal Counsel and the Office of the Deputy Attorney General (ODAG) in late 2003 and early 2004.[44] Among other concerns, Yoo did not address the 15-day warrant requirement exception in FISA following a congressional declaration of war. See 50 U.S.C. § 1811. Yoo's successors in the Office of Legal Counsel criticized this omission in Yoo's memorandum because they believed that by including this provision in FISA, Congress arguably had demonstrated an intention to "occupy the field" on the matter of electronic surveillance during wartime.[45] ~~(TS//STLW//SI//OC/NF)~~

Yoo's memorandum next analyzed Fourth Amendment issues raised by the Presidential Authorizations. Yoo dismissed Fourth Amendment concerns regarding the NSA surveillance program to the extent that the Authorizations applied to non-U.S. persons outside the United States. Regarding those aspects of the program that involved interception of the international communications of U.S. persons in the United States, Yoo asserted that Fourth Amendment jurisprudence allowed for searches of persons crossing the border and that interceptions of communications in or out of the United States fell within the "border crossing exception." Yoo further opined that electronic surveillance in "direct support of military operations" did not trigger constitutional rights against illegal searches and seizures, in part because the Fourth Amendment is primarily aimed at curbing law enforcement abuses. ~~(TS//STLW//SI//OC/NF)~~

Finally, Yoo wrote that the electronic surveillance described in the Presidential Authorizations was "reasonable" under the Fourth Amendment and therefore did not require a warrant. In support of this position, Yoo cited Supreme Court opinions upholding warrantless searches in a variety of contexts, such as drug testing of employees and sobriety checkpoints to detect drunk drivers, and in other circumstances "when special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable," *Veronia School Dist. 47J v. Acton*, 515 U.S. 464, 652 (1995) (as quoted in November 2, 2001, Memorandum at 20). Yoo wrote that in these situations the government's interest was found to have outweighed the individual's privacy interest, and that in this regard "no governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 435 U.S. 280, 307 (1981). According

---

[44] One of these officials was Patrick Philbin, who following Yoo's departure was "dual-hatted" as both an Associate Deputy Attorney General and a Deputy Assistant Attorney General in the Office of Legal Counsel. (U)

[45] We discuss the OLC's reassessment and criticism of Yoo's analysis in Chapter Four. (U)

to Yoo, the surveillance authorized by the Presidential Authorizations advanced this governmental security interest. ~~(TS//STLW//SI//OC/NF)~~

Yoo's memorandum focused almost exclusively on content interceptions. [redacted] ~~(TS//STLW//SI//OC/NF)~~ [redacted]

Yoo also omitted from his November 2 memorandum – as well as from his earlier September 17 and October 4, 2001, memoranda – any discussion of *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), a leading case on the distribution of government powers between the Executive and

[redacted]

46 [redacted]

Legislative branches.[47] As discussed in Chapter Four, Justice Jackson's analysis of President Truman's Article II Commander-in-Chief authority during wartime in the *Youngstown* case was an important factor in the Office of Legal Counsel's reevaluation in 2004 of Yoo's opinion on the legality of the Stellar Wind program. ~~(TS//SI//NF)~~

3. Additional Presidential Authorizations (U)

On November 30, 2001, the President signed a third Authorization authorizing the Stellar Wind program. The third Authorization was virtually identical to the second Authorization of November 2, 2001, in finding that the threat of terrorist attacks in the United States continued to exist, the legal authorities cited for continuing the electronic surveillance, and the scope of collection. ~~(TS//STLW//SI//OC/NF)~~

OLC Principal Deputy and Acting Assistant Attorney General Bradbury told the OIG that [redacted] Accordingly, the fourth Presidential Authorization, signed on January 9, 2002, modified the scope of collection to provide:

[redacted]

[47] In *Youngstown*, the Supreme Court held that President Truman's Executive Order directing the Secretary of Commerce to seize and operate steel plants during a labor dispute to produce steel needed for American troops during the Korean War was an unconstitutional exercise of the President's Article II Commander-in-Chief authority. In a concurring opinion, Justice Jackson listed three categories of Presidential actions against which to judge the Presidential powers. First, "[w]hen the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum[.]" Id. at 635. Second, Justice Jackson described a category of concurrent authority between the President and Congress as a "zone of twilight" in which the distribution of power is uncertain and dependant on "the imperatives of events and contemporary imponderables rather than on abstract theories of law." Id. at 637 (footnote omitted). Third, "[w]hen the President takes measures incompatible with the express or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter." Id. Justice Jackson concluded that President Truman's actions fell within this third category, and thus "under circumstances which leave Presidential power most vulnerable to attack and in the least favorable of possible constitutional postures." Id. at 640. (U)

[redacted]

Presidential Authorization, January 9, 2002. ~~(TS//STLW//SI//OC/NF)~~

[redacted] The language of the Authorization as modified in January 2002 remained the collection standard in subsequent Presidential Authorizations extending the Stellar Wind Program, until the disputed Presidential Authorization in March 2004, which we discuss in Chapter Four. ~~(TS//STLW//SI//OC/NF)~~

4. Subsequent Yoo Opinions (U)

In a 2-page memorandum to Attorney General Ashcroft dated January 9, 2002, Yoo wrote that [redacted] did not affect the legality of the Authorization. ~~(TS//STLW//SI//OC/NF)~~

Several identical Presidential Authorizations recertifying the Stellar Wind program were signed in 2002. (U//~~FOUO~~)

In October 2002, at Attorney General Ashcroft's request, Yoo drafted another opinion for Ashcroft concerning the Stellar Wind program. This memorandum, dated October 11, 2002, reiterated the same basic analysis in Yoo's November 2, 2001, memorandum in support of the legality of the Stellar Wind program.[48] [redacted]

[48] As in the November 2, 2001, memorandum, Yoo's October 11, 2002, memorandum included the following caveat: "Because of the highly sensitive nature of this subject and its level of classification, this memorandum has not undergone the usual editing and review process for opinions that issue from our Office [OLC]." ~~(TS//STLW//SI//OC/NF)~~

[redacted]

~~(TS//STLW//SI//OC/NF)~~

[redacted]

5. Yoo's Communications with the White House (U)

As the only Office of Legal Counsel official who had been read into the Stellar Wind program through early 2003, Yoo consulted directly with White House officials about the program during this period. Because we were unable to interview Yoo, we could not determine the exact nature and extent of these consultations. We were also unable to determine whether Ashcroft was fully aware of the advice Yoo was providing directly to the White House about the program. ~~(S//NF)~~

Gonzales told the OIG that Yoo was among those with whom the White House consulted to develop advice for the President on the program, but he asserted that Yoo was not sought out to provide approval of the program for the Department. However, Gonzales told us that he did not know how Yoo came to be the primary Justice Department official that the White House consulted during this period about the program. ~~(S//NF)~~

In fact, Jay Bybee, who served as the OLC Assistant Attorney General for most of this period and was Yoo's supervisor, was never read into the Stellar Wind program. Bybee told the OIG that during his tenure as Assistant Attorney General he did not know that Yoo was working alone on a sensitive compartmented program and he had no knowledge of how Yoo

came to be selected for this responsibility. Bybee told us that he was "surprised" and "a little disappointed" to learn in media accounts that he was not privy to Yoo's work on what Bybee had later learned to be a compartmented counterterrorism program involving warrantless electronic surveillance. Bybee said that it would not be unusual for a Deputy Assistant Attorney General such as Yoo to have direct contact with the White House for the purpose of rendering legal advice, but that the OLC Assistant Attorney General must be aware of all opinions that issue from the OLC. Bybee said that the Assistant Attorney General has an obligation to "see the whole picture" and is the person in the office who knows the full range of issues that are being addressed by the OLC and who can assure that OLC opinions remain consistent. ~~(TS//SI//NF)~~

6. Gonzales's View of the Department's Role in Authorizing the Stellar Wind Program ~~(S//NF)~~

The OIG asked Gonzales about how he, as White House Counsel, viewed the role of the Justice Department during the early phase of the Stellar Wind program. Gonzales stated that he and others at the White House tried to be very careful to understand what could be done legally, and they wanted to have "constant communications with the Department" in the first few months following the September 11, 2001, terrorist attacks. Gonzales also stated that it was the President, and not the Attorney General or the White House Counsel, who authorized the warrantless surveillance activity under the Stellar Wind program. However, Gonzales acknowledged that the President's decision was based on advice from the Attorney General and White House Counsel, among others. ~~(TS//SI//NF)~~

The OIG also asked whether Gonzales had a personal belief about the justification for having a single attorney – Yoo – speak on behalf of the Department regarding the legality of the program. Gonzales stated that it was up to the Attorney General to make that determination or calculation. Gonzales stated that he understood the Department's position was that the program was legal and that Yoo would sit down with Attorney General Ashcroft to answer any legal questions when the Presidential Authorizations were presented to Ashcroft for his signature. Gonzales said he understood that the Yoo opinions represented the legal opinion of the Department. However, as noted previously, for the first year and a half of the program the Department read-ins included only Yoo, Ashcroft, and Baker. ~~(TS//SI//NF)~~

Gonzales also stated that it was Ashcroft's decision as to how to satisfy his legal obligations as Attorney General. However, when the OIG asked whether Gonzales was aware if Ashcroft ever requested to have additional people read into Stellar Wind, Gonzales stated that he recalled Ashcroft wanted Deputy Attorney General Larry Thompson and his Chief of Staff, David Ayres, read in. Gonzales acknowledged that neither official was

ever read into the program. Gonzales said that Ashcroft complained that it was "inconvenient" not to have Thompson and Ayres read in, but Gonzales also stated that he never got the sense from Ashcroft that it affected the quality of the legal advice the Department provided to the White House. Gonzales stated that other than Ashcroft's request that Thompson and Ayres be read in, he did not recall Ashcroft requesting to have additional Department officials read in.[49] ~~(S//NF)~~

II. NSA's Implementation of the Stellar Wind Program (U//~~FOUO~~)

In this section, we describe the NSA's initial implementation of the Stellar Wind program. We first describe how the NSA acquired the communications data authorized for collection under the program. We also discuss the process the NSA used to analyze the information received from the Stellar Wind program and how this information was provided to the FBI. (U//~~FOUO~~)

A. Implementation of Stellar Wind (U//~~FOUO~~)

Our description of the implementation of the Stellar Wind program is based on NSA and Justice Department documents we obtained during our review, as well as interviews of NSA and Department personnel with knowledge of Stellar Wind's technical operation. This section provides a basic overview of how the NSA obtained [redacted] the information authorized for collection under Stellar Wind. This information is also important for later sections of this report that describe significant modifications to the Authorizations regarding the manner and scope of collection, the Department's re-assessment of the legal rationale supporting the Stellar Wind program during late 2003 and early 2004, and compliance issues that arose when the Department decided to seek collection of [redacted] ~~(TS//STLW//SI//OC/NF)~~ [redacted]

[49] Gonzales stated that Ashcroft, as the Attorney General, would be well-positioned to request the President to allow additional attorneys to be read into the program. Drawing on his own experience as Attorney General, Gonzales cited his request to the President in 2006 that the then head of the Office of Professional Responsibility (OPR) and several attorneys within OPR be granted security clearances in order to conduct an inquiry into the professional conduct of Department lawyers with respect to the Stellar Wind program. Gonzales said he made his request both through White House Counsel Harriet Miers and directly to the President. However, the President initially declined the request, and the request was not granted until October 2007. (U//~~FOUO~~)

[redacted]

[redacted] As discussed previously, the NSA collected three categories of information under Stellar Wind that came to be commonly referred to as the three "baskets." Basket 1 referred to collection of the content of telephone and e-mail communications; basket 2 referred to collection of meta data associated with telephone communications; and basket 3 referred to collection of meta data associated with e-mail and other Internet communications. [redacted]

[redacted].[52] ~~(TS//STLW//SI//OC/NF)~~

---

[50] [redacted]

[51] We describe in Chapter Four changes made in March and [redacted] 2004 [redacted] under Presidential Authorization following a dispute between the White House and Justice Department concerning the legality of the Stellar Wind program. [redacted] ~~(TS//SI//NF)~~

[52] Title 18 of the United States Code generally prohibits the interception and disclosure of wire, oral, or electronic communications, and provides for criminal penalties for any person engaging in such activity. See 18 U.S.C. § 2511. [redacted]

[redacted]

The meta data collected [redacted] under Stellar Wind (baskets 2 and 3), as well as the meta data associated with communications targeted for content collection under the program, was placed into an NSA database system called [redacted] which according to NSA officials is a configuration of databases and analytical tools. [redacted] databases are segregated into "realms" organized by the specific authority allowing the particular data to be collected.[53] The content data collected under the Stellar Wind program was placed in a separate NSA repository.[54] ~~(TS//STLW//SI//OC/NF)~~

1. Basket 1 – Telephone and E-Mail Content Collection ~~(TS//STLW//SI//OC/NF)~~

a. Telephone Communications (U)

In this section we describe briefly the technical means used by the NSA to access the international telephone system to accomplish the collection of international calls under the Stellar Wind program.[55] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

(U)

[redacted]

[53] NSA officials said the realms also establish a system of access control to ensure that only authorized users access certain data. ~~(S//NF)~~

[54] As discussed in Chapter Five of this report, the NSA created an additional realm in July 2004 when the government obtained FISA authority to collect e-mail meta data, and another realm in May 2006 when it obtained authority under FISA to collect telephony meta data. These realms were separate from the realms that contained information collected under Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

[55] The NSA's interception of international telephone communications under Stellar Wind highlighted the dramatic change in telecommunications technology that had been taking place for nearly 20 years. In 1978, when FISA was enacted, telephone calls placed by and to individuals within the United States (domestic calls) were carried mostly on copper wires, while telephone calls placed to or from individuals outside the United States (international calls) generally were transmitted by satellites. FISA reflected the state of technology then by defining the term "electronic surveillance" to be the acquisition of the contents of certain wire and radio (satellite) communications. FISA stated that as to radio

(Cont'd.)

[redacted]

communications specifically, and thus as to most international communications, the interception of calls constituted "electronic surveillance" only if the acquisition intentionally targeted a particular known U.S. person in the United States, or if all participants to the communication were located in the United States. See 50 U.S.C. §§ 1801(f)(1) and (3). Accordingly, government surveillance that targeted foreign persons outside the United States generally was not considered electronic surveillance under FISA, and the government was not required to obtain a FISA Court order authorizing the surveillance even if one of the parties to the communication was in the United States.
~~(TS//STLW//SI//OC/NF)~~

[redacted]

56 [redacted]

[redacted]

b. E-Mail Communications ~~(TS//SI//NF)~~

[redacted]

57

[redacted]

[redacted]

[redacted] However, under the October 4, 2001, Presidential Authorization, the NSA for the first time was authorized to intercept international e-mails originating or terminating inside the United States. [redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[redacted]

[redacted]

[redacted]

2. Basket 2 – Telephony Meta Data Collection ~~(TS//STLW//SI//OC/NF)~~

[redacted]

60 [redacted]

The NSA informed the FISA Court of this issue in the government's December 2006 FISA application that sought to bring Stellar Wind's content collection under FISA authority (discussed in Chapter Five of this report). [redacted]

~~(TS//STLW//SI//OC/NF)~~

[redacted] These records, also referred to as call detail records, consist of routing information that includes the originating and terminating telephone number of each call, and the date, time, and duration of each call. The call detail records do not include the substantive content of any communication or the name, address, or financial information of a subscriber or customer. ~~(TS//STLW//SI//OC/NF)~~

As discussed above, the initial Presidential Authorizations [redacted] that is, call detail records pertaining to communications where at least one party was outside the United States, where no party was known to be a United States citizen, or where there was reasonable articulable suspicion to believe the communication related to international terrorism. As noted in Chapter One, the NSA interpreted this authority to also permit it to collect telephony and e-mail meta data in bulk so that it would have a database from which to acquire the targeted meta data. [redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

61 [redacted]

62 [redacted]

(Cont'd.)

[redacted]

[redacted] The NSA personnel also organized the data into a format that could be used by NSA analysts responsible for analyzing the information under the Stellar Wind program. The data was archived into an NSA analytical database that contained exclusively Stellar Wind information and that was accessible only by specially authorized NSA personnel read into the program. ~~(TS//STLW//SI//OC/NF)~~

[redacted][63] While the magnitude of the bulk collection was enormous, the NSA did not retrieve or review most of this data because access was authorized only with respect to telephone communications that satisfied the Presidential Authorizations "acquisition" standard. In fact, the NSA reported that by the end of 2006, .001% of the data collected had actually been retrieved from its database for analysis. ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[63] We describe these techniques in part B of this section. (U)

3. Basket 3 – E-Mail Meta Data Collection
~~(TS//STLW//SI//OC/NF)~~

[redacted]

The meta data the NSA obtained from e-mail communications included the information that appeared on the "to," "from," "cc," "bcc," and "sent" lines of a standard e-mail. Thus, the NSA collected the e-mail address of the sender, the e-mail addresses of any recipients, and the information concerning the date and time when the e-mail was sent.
~~(TS//STLW//SI//OC/NF)~~

[redacted] The meta data collection did not include information from the "subject" or "re" lines of the e-mails or the body of the e-mails.[64]
~~(TS//STLW//SI//OC/NF)~~

64 [redacted]

[redacted] ~~(TS//STLW//SI//OC/NF)~~

B. NSA Process for Analyzing Information Collected Under Stellar Wind ~~(S//NF)~~

The NSA conducted two functionally distinct types of review of the massive amount of data it collected under the Stellar Wind program. First, the NSA conducted procedures intended to ensure that it only reviewed or "acquired" the information that was within the scope of the Presidential Authorizations. Second, the NSA conducted substantive analysis of the acquired information to determine whether it had intelligence value that should be disseminated to customer agencies such as the FBI and the CIA. ~~(TS//SI//NF)~~

The NSA procedures to ensure that the acquisition and dissemination standards were satisfied became more formalized over time. We describe below how the NSA handled the enormous volume of data it was collecting with the Stellar Wind program. ~~(TS//SI//NF)~~

1. Basket 1: Content tasking, Analysis, and Dissemination ~~(TS//STLW//SI//OC/NF)~~

Stellar Wind's "basket 1" content database contains telephone and e-mail communications of individuals. The NSA refers to the telephone numbers and e-mail addresses tasked for interception as "selectors." To task a selector under the Presidential Authorizations, the NSA was required to establish probable cause to believe the intercepted communications originated or terminated outside the United States and probable cause to believe a party to the communications was a group engaged in international terrorism, or activities in preparation therefor, or any agent of such a group.[65] ~~(TS//STLW//SI//OC/NF)~~

The NSA had two processes for tasking selectors under Stellar Wind. One process applied to tasking foreign selectors, or selectors believed to be

[65] [redacted]

used by non-U.S. persons outside the United States. The other process applied to tasking domestic selectors, or selectors believed to be used by persons inside the United States or by U.S. persons abroad. A foreign selector could be tasked for collection under Stellar Wind based upon an NSA analyst's determination, following some amount of documented research and analysis about the selector, that the terms of the Authorizations were satisfied. The NSA did not require any additional levels of approval before a foreign selector could be tasked.[66]
~~(TS//STLW//SI//OC/NF)~~

A domestic selector could be tasked only after the NSA analyst obtained specific approvals. The rigor of the process to task a domestic selector evolved over time, but essentially it required an analyst to draft a formal tasking package that demonstrated, through analysis and documentation, that the selector satisfied the terms of the Authorizations. This package was reviewed by a designated senior official who could approve or reject the package, or request that additional information be provided.
~~(TS//STLW//SI//OC/NF)~~

In emergency situations, the NSA could commence content interception on a selector within [redacted] of identifying a number or address that satisfied the criteria in the Presidential Authorizations. In other cases, interception commenced within [redacted] for urgent or priority taskings and within a week for routine taskings. ~~(TS//STLW//SI//OC/NF)~~

The NSA conducted 15-, 30-, and 90-day reviews of tasked foreign and domestic selectors to assess whether the interception should continue. The NSA stated that the selectors were "de-tasked" if the user was arrested, if probable cause could no longer be established, or if other targets took priority. ~~(TS//STLW//SI//OC/NF)~~

The content intercepted under taskings was sent to the NSA and placed in a database accessible by NSA analysts cleared into the Stellar Wind program. The analysts were responsible for reviewing the communications and assessing whether a Stellar Wind report should be generated for the FBI and the CIA. [redacted]

[redacted]

[redacted]

~~(TS//STLW//SI//OC/NF)~~

2. Baskets 2 and 3: Telephony and E-Mail Meta Data Queries, Analysis, and Dissemination ~~(TS//STLW//SI//OC/NF)~~

The NSA received [redacted] a massive amount of telephony and e-mail meta data (basket 2 and 3 information) that was stored in a realm accessible only by NSA analysts assigned to the Stellar Wind program. The purpose of the collection was to facilitate the identification of connections [redacted] among particular telephone numbers and e-mail addresses by using [redacted] sophisticated analytical techniques called "contact chaining" [redacted] ~~(TS//STLW//SI//OC/NF)~~

As described by the NSA in declarations filed with the FISA Court, contact chaining is used to determine the contacts made by a particular telephone number or e-mail address (tier one contacts), as well as contacts made by subsequent contacts (tier two and tier three contacts). The NSA uses computer algorithms to identify the first two tiers of contacts an e-mail address makes and the first three tiers of contacts a telephone number makes. According to the NSA, multi-tiered contact analysis is particularly useful with telephony meta data because a telephone does not lend itself to simultaneous contact with large numbers of individuals as e-mail does with spam. [redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

As previously noted, the NSA interpreted the Presidential Authorizations to permit it to collect telephony and e-mail meta data in bulk.[67] The NSA "queried" the databases that held this data to identify meta data for communications to or from a particular telephone or e-mail address (the "selector," also known as the "seed number" or "seed account"). NSA analysts queried the database using a selector for which there was a reasonable articulable suspicion to believe that the number or account had been used for communications related to international terrorism.[68] [redacted]

[redacted]

~~(TS//STLW//SI//OC/NF)~~

[redacted]

As with proposals to task selectors, an NSA shift coordinator typically reviewed for approval proposals to query either the e-mail or telephony meta data bulk databases using particular selectors. If the shift coordinator agreed that the reasonable articulable suspicion standard was met, the selector was approved and the analyst was authorized to query the meta data bulk database to identify all of the other telephone numbers or e-mail addresses that had been in contact with the seed account. Each contact along the chain of contacts that originated with the selector was referred to as a "hop," meaning that a telephone call from the seed account to telephone number A was considered "one hop out," and a call from telephone number A to telephone number B was considered "two hops out" (relative to the seed account), and so on. NSA analysts used specialized software to chain and analyze the contacts identified by each query. The

67 [redacted]

68 [redacted]

NSA told us that Stellar Wind analysts were permitted to chain the results of queries up to three hops out from the selector. ~~(TS//STLW//SI//OC/NF)~~

The results of each query were analyzed to determine whether any of the contacts should be reported, or "tipped," to Stellar Wind customers – primarily the FBI, CIA, and the National Counterterrorism Center. In the first months of the Stellar Wind program, the NSA reported to the FBI most contacts identified between a U.S. telephone number or e-mail address and the selector used to query the meta data realm, as well as domestic contacts that were two and three hops out from a selector. As discussed in Chapter Six of this report, over time the NSA and FBI worked to improve the reporting process and the quality of the intelligence being disseminated under Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

The domestic contacts from specified numbers or e-mail addresses, called "tippers," were provided to the FBI by the NSA. These tippers were included in reports that contained two sections separated by a dashed line, commonly referred to as a "tearline," made to appear as a perforation extending across the width of a page. The purpose of the tearline was to separate the compartmented information above the tearline, which could identify the specific sources and methods used to obtain the information, from the non-compartmented information that the FBI could further disseminate to its field offices. Only FBI personnel read into the Stellar Wind program could have access to the full Stellar Wind reports from NSA. ~~(TS//STLW//SI//OC/NF)~~

The information that appeared above the tearline typically was classified Top Secret/SCI and identified Stellar Wind as the source of the intelligence. The information included specific details [redacted] as well as any pertinent comments by NSA intelligence analysts. ~~(TS//STLW//SI//OC/NF)~~

The information that appeared below the tearline of a report generally was classified Secret or Confidential and did not identify Stellar Wind as the source of the intelligence. The text typically included some version of the following statement:

[redacted]

The amount of information about the contacts that followed this statement varied. [redacted]

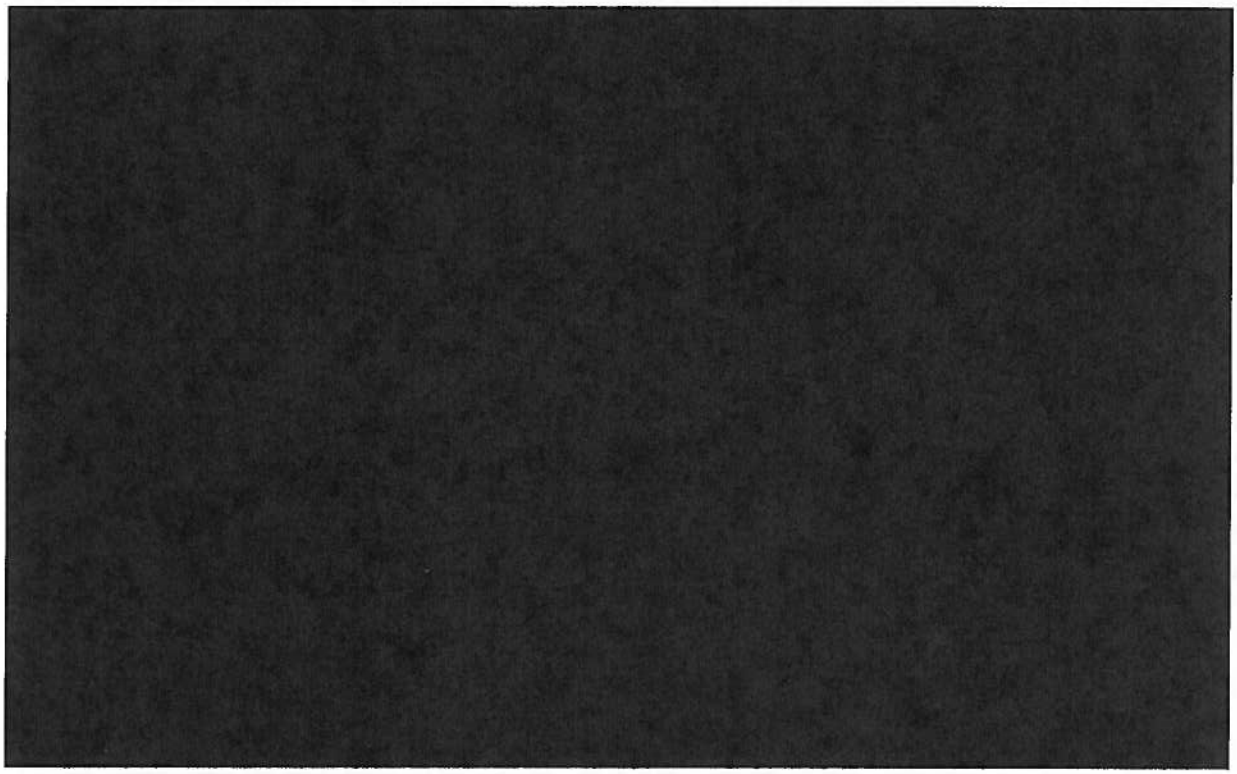
[redacted] and provided the date or dates of the contacts, or the period of time in which contact was made. ~~(TS//STLW//SI//OC/NF)~~

During the first several months of the Stellar Wind program, nearly all reports based on telephone or e-mail meta data analysis designated each of the tippers as [redacted]

~~(TS//STLW//SI//OC/NF)~~

As examples, the following Stellar Wind reports were among those disseminated to the FBI in November 2001. We have excerpted only the information below the tearline, which is often referred to simply as "tearline information." In addition, we did not provide the actual telephone numbers provided by the NSA to the FBI. ~~(TS//SI//NF)~~

[redacted]



III. FBI's Early Participation in the Stellar Wind Program ~~(S//NF)~~

Stellar Wind was not an FBI program, nor was the FBI involved in the program's creation. However, as the lead agency for counterterrorism in the United States, the FBI received much intelligence produced under Stellar Wind. In the following sections, we describe how the FBI became involved in the Stellar Wind program, the personnel resources allocated to handle Stellar Wind information, and the initial procedures the FBI established to receive, control, and disseminate the program information. ~~(TS//STLW//SI//OC/NF)~~

---

[69] In addition to the queries the NSA conducted on a case-by-case basis, the NSA also maintained a list of foreign and domestic telephone numbers and e-mail addresses for which, based on NSA analysts' assessments, there was a reasonable basis to believe were associated with international terrorism. These selectors, called "alerts," were queried against the incoming meta data automatically on a daily basis, and any contacts with a domestic telephone number or e-mail address were directed to NSA analysts for review and possible reporting to the FBI. The NSA regularly updated the alert list by adding or removing selectors, depending on the available intelligence. As we discuss in Chapter Five in connection with the transition of Stellar Wind's bulk meta data collection from presidential authority to FISA authority, the FISA Court found that the NSA's use of the alert list to query incoming telephone meta data did not comply with terms of the Court's Order. ~~(TS//STLW//SI//OC/NF)~~

A. FBI Director First Informed of Stellar Wind Program (U//~~FOUO~~)

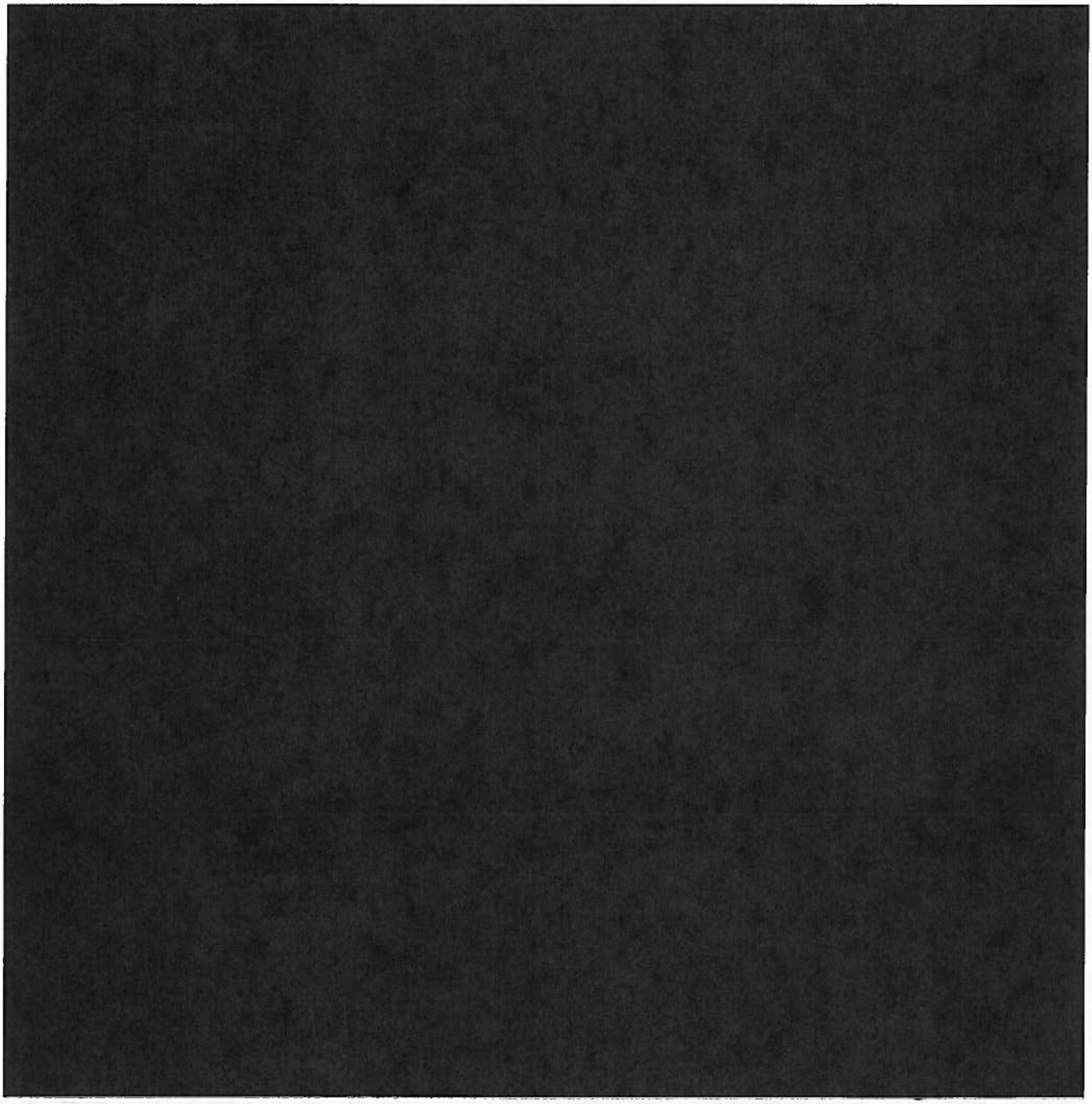
Director Mueller told us that his earliest recollection of the Stellar Wind program was a meeting he attended at the White House with Attorney General Ashcroft, which occurred either after the decision had been made to move forward with the presidentially authorized program or shortly after the October 4, 2001, Authorization was issued. Mueller told us the meeting was "more than a formal read-in" and that Director Hayden may have attended. Mueller said that at or around this time he also briefly reviewed the October 4, 2001, Presidential Authorization, which he characterized as "relatively complex." ~~(TS//SI//OC/NF)~~

Director Mueller said his impression at the time was that the terms of the Presidential Authorization might allow for collecting purely domestic telephone and e-mail communications. Mueller said he discussed the matter with Ashcroft and asked whether OLC had issued an opinion on the program. Mueller said that he recalled being told that OLC might have opined orally on the program and Mueller said he suggested to Ashcroft that OLC issue a formal written opinion. Mueller told us that he did not think the NSA ever exercised authority under the Authorization to collect purely domestic communications. ~~(TS//STLW//SI//OC/NF)~~

Mueller stated that based on the meeting he attended at the White House and his brief review of the October 4, 2001, Presidential Authorization, he understood the FBI's role in the Stellar Wind program was to be a "recipient" of intelligence generated by the NSA, and to provide any technical support to the NSA as necessary to support the program. ~~(TS//SI//NF)~~

B. [redacted]

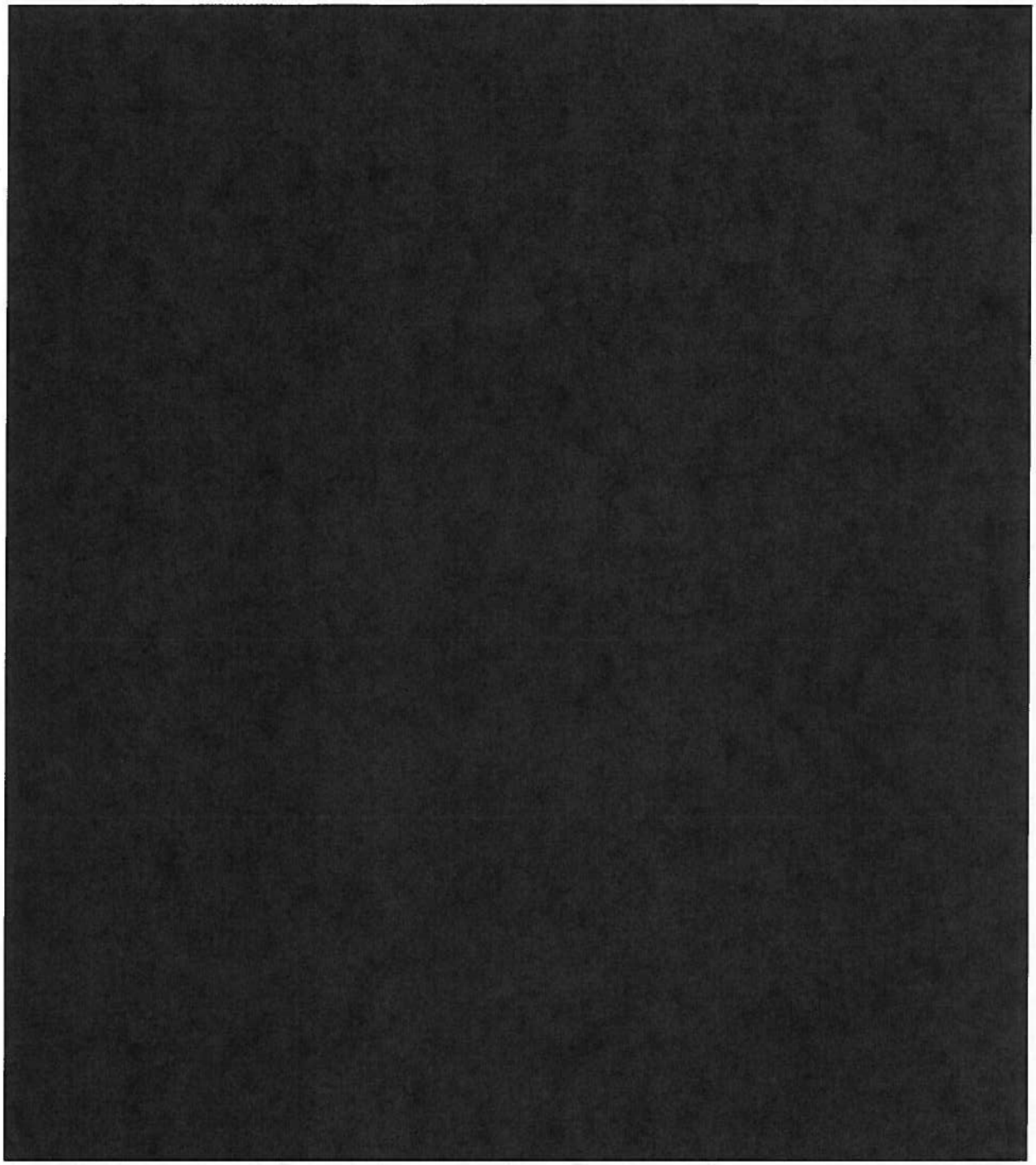
[redacted]



[redacted]

[70] Executive Order 12333 authorizes the FBI to provide operational support to the Intelligence Community. (U)

[71] [redacted]



Mueller said he therefore decided to request an order from the

Attorney General formally directing the FBI to support the NSA program. Mueller said that he also requested the order because he wanted a "record as to our participation." ~~(TS//STLW//SI//OC/NF)~~

In response, on October 20, 2001, Attorney General Ashcroft sent a memorandum to Director Mueller stating:

> As part of the Nation's self defense activities, the National Security Agency (NSA) is engaged in certain additional collection activities, the details of which you are aware. Those activities are legal and have been appropriately authorized, and the Federal Bureau of Investigation should cooperate with NSA as necessary for it to conduct those activities. ~~(TS//SI//NF)~~

According to Mueller, the combination of this memorandum from the Attorney General and the November 2, 2001, memorandum prepared by the Department's Office of Legal Counsel regarding the legality of Stellar Wind gave him comfort at that time with the FBI's participation in the program. ~~(TS//SI//NF)~~

[redacted]

Bowman also told us that the White House officials primarily responsible for Stellar Wind, who he identified as the Vice President and Addington, were "amateurs" when it came to intelligence work. Bowman stated that one of the potential consequences of severely limiting the number of individuals read into a program is that uncleared personnel who

occupy positions placing them in close proximity to program-related activities might construe certain actions as questionable or illegal and report that activity, thereby potentially compromising the activities. Bowman said that this is what occurred with Stellar Wind. For this reason and others, Bowman did not agree with the decision to so severely limit access to the program. ~~(TS//STLW//SI//OC/NF)~~

[redacted]

C. FBI Begins to Receive and Disseminate Stellar Wind "Tippers" ~~(S//NF)~~

In the immediate aftermath of the September 11 terrorist attacks, the FBI had created a task force of agents and analysts to analyze the flood of telephone numbers it received from multiple sources, including agencies within the U.S. Intelligence Community, foreign intelligence services, and concerned citizens. The task force, called the Telephone Analysis Unit (TAU), was located at FBI Headquarters and consisted of approximately 50 FBI employees working on shift rotations 24 hours per day, 6 days per week. The operation was supervised by FBI supervisors working out of the FBI's Strategic Information and Operations Center. As described below, personnel assigned to this task force were among the first at the FBI to handle Stellar Wind-derived information. ~~(TS//STLW//SI//OC/NF)~~

1. FBI Initiates [redacted] ~~(S//NF)~~

In October or November 2001, several TAU analysts were assigned to what came to be called the [redacted] which was the FBI's effort to manage the Stellar Wind-derived information being received from the NSA. The information, referred to as Stellar Wind "tippers," consisted of telephone numbers and e-mail accounts derived from NSA meta data analysis, and sometimes content intercepted from particular telephone and e-mail communications. The essential purpose of the [redacted] was to receive Stellar Wind tippers from the NSA and disseminate the information to FBI field offices for investigation in a manner that did not reveal the source of the information or the methods by which it was collected. ~~(TS//STLW//SI//OC/NF)~~

Working alternating shifts in the FBI's Strategic Information and Operations Center, two FBI analysts were primarily responsible for managing Stellar Wind tippers in the initial months of the program. These analysts told the OIG that until December 2001, the Stellar Wind tippers

consisted nearly exclusively of telephone numbers. According to the analysts, the process for handling Stellar Wind tippers began when the NSA liaison co-located at FBI Headquarters provided one of the analysts the information below the tearline from a Stellar Wind report containing one or more tippers. The analyst then queried FBI databases for any information about each tipper, such as whether the tipper appeared in any pending or closed FBI investigations. The analyst also queried the tipper against the FBI's [redacted] database, which is the FBI's central repository for telephone subscriber data acquired during the course of investigations. In addition, the analyst checked each tipper against public source databases for relevant information, such as the identity of a telephone number subscriber. ~~(TS//STLW//SI//OC/NF)~~

After completing these database checks, the analyst drafted an Electronic Communication, or EC, from FBI Headquarters to the appropriate FBI field office. The EC described the tearline information about the tipper contained in the Stellar Wind report together with any additional information the analyst was able to locate. ~~(TS//STLW//SI//OC/NF)~~

The [redacted] ECs disseminated to field offices included several features concerning the nature of the information and how it could be used. First, the ECs advised the field offices that the information being provided was "derived from an established and reliable source" and that it was "being addressed by the TAU as the [redacted]"[72] ~~(S//NF)~~

Second, the ECs included a caveat about the use of the information being provided, stating that the information "is for lead purposes only and is intended solely for the background information of recipients in developing their own collateral leads. It cannot be used in affidavits, court proceedings, subpoenas, or for other legal or judicial purposes." The FBI said this language was included in each EC to protect the source of the information and the methods by which it was collected. ~~(S//NF)~~

Third, the ECs provided an explanation about the qualitative rankings assigned to the tippers. As described previously, the NSA assigned each tipper a [redacted] ranking [redacted][73] ~~(TS//SI//NF)~~

72 [redacted] ~~(S//NF)~~

73 [redacted]

(Cont'd.)

Fourth, the ECs instructed the field offices how the tippers should be addressed. These instructions were provided as "leads," for which the FBI had three categories: Action, Discretionary, and For Information. An Action lead instructed a field office to take a particular action in response to the EC. An Action lead was "covered" when the field office took the specified action or conducted appropriate investigation to address the information in the EC. A Discretionary lead allowed the field office to take whatever action it deemed appropriate. A field office that receives a "For Information" lead was not expected to take any specific action in response to the EC other than possibly route the communication to the office personnel whose investigations or duties the information concerned. ~~(S//NF)~~

After the FBI analyst completed this process and drafted the EC, an FBI Supervisory Special Agent read into the Stellar Wind program reviewed the EC, in part to ensure that it did not reveal the source of the information or the method by which the information was obtained. Once approved, the analyst entered the EC into the FBI's Automated Case Management System and the receiving field offices were notified electronically to review the communication. ~~(TS//SI//NF)~~

Each [redacted] EC typically contained multiple tippers and therefore was distributed to multiple field offices. The receiving field offices were responsible for handling the leads that concerned tippers falling in their respective geographic jurisdictions. ~~(S//NF)~~

Most of the [redacted] leads that disseminated Stellar Wind tippers were designated Action leads. As noted, during this period the tippers were almost exclusively telephone numbers. Accordingly, the typical lead instructed the field office to [redacted] The lead also instructed the field office to report the investigative results to the Telephone Analysis Unit. ~~(TS//SI//NF)~~

The two [redacted] analysts told us that the focus of their work in the first months after the September 11 attacks was to detect what many believed was an imminent second attack. During this period, nearly all of the Stellar Wind tippers the FBI received were disseminated to a field office for investigation as quickly as possible. ~~(S//NF)~~

In addition to tippers containing the content of intercepted telephone and e-mail communications (content tippers), in approximately December

---

[redacted] ~~(TS//SI//NF)~~

2001 the NSA began providing the FBI tippers derived from the NSA's e-mail meta data analysis (e-mail tippers). These e-mail tippers initially were routed to the same two analysts who were managing the telephone tippers. The analysts told us that the e-mail tippers were processed and disseminated in the same manner as the telephone tippers. Content tippers, which according to the analysts were received very infrequently during this early period, generally were also disseminated by EC to the appropriate field offices, but little if any research regarding the information was conducted. The analysts said they considered the content tippers particularly time-sensitive and for that reason occasionally transmitted the ECs directly to the appropriate field offices or called the offices to advise that the information was being loaded into the FBI's Automated Case Management System. In 2002, responsibility for e-mail tippers was reassigned to the Electronic Communications Analysis Unit. ~~(TS//STLW//SI//OC/NF)~~

In February 2002, one of the two FBI analysts left the [redacted] after being selected for a management position in a different analytical section within the FBI's Counterterrorism Division. The remaining analyst became solely responsible for managing the Stellar Wind tippers under the [redacted] a situation that continued for approximately the next 12 months. The analyst told us that while her work hours during this period were "ridiculous," she did not feel there was any pressure to add analysts to the project because "the process was working well." ~~(TS//SI//NF)~~

In early 2002, FBI management instructed the lone [redacted] analyst to conduct some of her work while physically located in the NSA Headquarters at Fort Meade, Maryland. This created an unusual arrangement for the analyst. The analyst continued to receive the NSA's daily Stellar Wind reports at FBI Headquarters, and she would then drive to the NSA with the reports to draft the ECs (the analyst had remote access to FBI databases from an NSA workstation). The analyst told us that interaction with NSA counterparts during these daily visits was minimal. After the ECs were drafted, the analyst returned to FBI Headquarters to obtain approval to disseminate the communications to the FBI's field offices. The analyst's impression was that FBI management created this unusual arrangement "for show" and that its purpose was to establish an FBI "presence" at the NSA in connection with Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

The analyst continued working on Stellar Wind matters until approximately February 2003, when a small team of FBI personnel were

assigned permanently to the NSA to manage the FBI's participation in the Stellar Wind program.[74] ~~(S//NF)~~

2. FBI Field Offices' Response to [redacted] Leads ~~(S//NF)~~

According to the two FBI analysts responsible for managing Stellar Wind information under the [redacted] from approximately October 2001 to February 2003, some agents in FBI field offices grew frustrated with the information they were receiving under the program. Because the [redacted] ECs that disseminated the tippers to the field offices assigned most of them as Action leads, this required that the leads be covered expeditiously. ~~(S//NF)~~

Under ordinary operating procedures, investigative leads for international terrorism matters are set by FBI Headquarters' International Terrorism Operations Section. In addition, the ECs assigning international terrorism leads typically identified a Supervisory Special Agent within ITOS as the point-of-contact for any questions field offices might have. Because the Stellar Wind program was so tightly compartmented, the leads sent during this early period by the [redacted] were not coordinated with ITOS, and the FBI Headquarters point-of-contact identified in the ECs for any questions generally was one of the two [redacted] analysts. ~~(S//NF)~~

According to one of the [redacted] analysts, agents responsible for covering the Action leads complained that the lack of background information provided in the ECs about the tippers made it difficult to determine what investigative steps could or should be taken. [redacted][75] Consequently, the analyst

---

[74] This co-location of FBI personnel at the NSA is discussed below. ~~(S//NF)~~

[75] To open a full investigation, the FBI was required to [redacted] A preliminary inquiry required only a showing of [redacted] See Attorney General Guidelines for [redacted] The FBI's practice of issuing national security letters based on Stellar Wind-derived information is discussed in Chapter Six of this report. ~~(S//NF)~~

received calls from agents requesting additional information about the source of the intelligence provided in the ECs to help the agents decide whether there was sufficient predication to open an investigation on the telephone number or to issue a national security letter for subscriber information. ~~(TS//SI//NF)~~

The analyst stated that in response to these calls he could only reiterate to the agents that the information was provided by a reliable, sensitive source. The analyst said this situation produced a "dichotomy" with the tippers. On the one hand, there was a demand in the International Terrorism Operations Section and field offices for the telephone numbers because of their priority [redacted] status and the prevailing concern that there would be a second terrorist attack; on the other hand, the limited and vague information contained in the [redacted] ECs caused some confusion and frustration among agents investigating the lead. ~~(S//NF)~~

Agents also complained that many tippers were already known to the FBI from past or pending investigations and that the [redacted] ECs were providing "circular reporting."[76] However, according to one [redacted] analyst, this generally did not occur. The analyst explained that an agent in the field assigned to cover a lead on a telephone number did not know the NSA was the source of the intelligence. Consequently, when the agent discovered that the number was identical to a number the agent was already investigating or was aware of, it appeared to the agent that the [redacted] simply had identified a previously known number, conducted some additional research that the field office likely had already done, and disseminated the information back to the field as new reporting. Because the analysts could not fully explain the source of the intelligence, the agent did not realize the [redacted] reporting in fact reflected a new foreign connection to the telephone number. ~~(TS//STLW//SI//OC/NF)~~

Another frustration voiced by agents to the [redacted] analysts was that leads disseminated under the project that were designated "Action leads" frequently did not yield significant investigative results, such as identifying new persons of interest or contributing to an active investigation. [redacted]

[76] For example, circular reporting might have occurred when the FBI passed a Stellar Wind-derived telephone number or e-mail address to another agency within the U.S. Intelligence Community, that agency in turn requested the NSA to analyze the information, and the NSA subsequently disseminated the results back to the FBI in a Stellar Wind report. ~~(TS//STLW//SI//OC/NF)~~

[redacted]

~~(TS//STLW//SI//OC/NF)~~

The NSA responded to this frustration by implementing the [redacted] rankings described earlier to provide the agents some guidance on prioritizing the tippers. In addition, the FBI analysts told us that they became more adept at telephone analysis and "got better at their game" by eliminating low value tippers [redacted] from being disseminated to field offices. According to FBI documents, the FBI also sought additional information from the NSA about tippers ranked [redacted] before the FBI disseminated these tippers to the field for investigation. ~~(TS//STLW//SI//OC/NF)~~

3. FBI's Efforts to Track Stellar Wind Tippers and Update Executive Management on Status of [redacted] Leads ~~(S//NF)~~

Typically, FBI ECs originate from a specific investigative or administrative case file number. A file number is also required for an EC to be loaded into the FBI's Automated Case Management System and to enable the sending office to assign a lead to the receiving office. However, FBI Headquarters did not initially open an investigative file for the [redacted] ECs that disseminated Stellar Wind tippers to field offices. One of the original analysts assigned to the project told the OIG that he was familiar with a telephone analysis project in the FBI's drug program and that as a result he decided to issue the first Stellar Wind-related EC from that drug investigative file. This confused some field offices receiving the earliest ECs because counterterrorism leads were being disseminated under a drug investigation file number. ~~(TS//STLW//SI//OC/NF)~~

In mid-October 2001, the FBI created a subfile under the FBI's investigation of the September 11 terrorist attacks to disseminate Stellar Wind information. The FBI used this subfile, referred to as the [redacted] until September 2002, when a more formal program for disseminating Stellar Wind information, called [redacted] was created.[77] ~~(TS//STLW//SI//OC/NF)~~

The [redacted] analysts also told us that they created a database to attempt to track the status of leads disseminated to the field offices. The database identified each tipper by field office and the status of the lead that was assigned. One analyst stated that the response rate from

[77] We describe this more formal program in Chapter Six of this report. (U)

field offices was uneven during these early months, and their supervisors instructed the analysts at one point to contact the head of each field office to determine the status of the [redacted] leads for which each office was responsible. ~~(S//NF)~~

The [redacted] analysts used the database they created to produce status reports for senior FBI officials who were read into the Stellar Wind program. These reports provided statistics regarding the quantity and rankings of disseminated tippers, as well as brief synopses of the status of the [redacted] leads. The Stellar Wind program was viewed as an emergency response to the September 11 attacks and these status reports were intended to provide FBI executives information about how the program was contributing to the FBI's counterterrorism efforts. ~~(TS//SI//NF)~~

IV. Justice Department Office of Intelligence Policy and Review's (OIPR) and FISA Court's Early Role in Stellar Wind ~~(TS//STLW//SI//OC/NF)~~

When the President signed the first Authorization for the program on October 4, 2001, only two Department officials outside the FBI were read into the Stellar Wind program: Attorney General John Ashcroft, who certified the Authorization as to form and legality; and John Yoo, the Deputy Assistant Attorney General in the Office of Legal Counsel responsible for advising the Attorney General on the matter and for drafting the Department's first memorandum on the legality of the program.[78] The Department's Office of Intelligence Policy and Review (OIPR), despite its expertise in FISA matters, was not asked to consider how FISA might affect the program's legality or implementation, nor was OIPR asked to consider how the program might affect the Department's FISA operations. ~~(TS//SI//NF)~~

In this section, we provide an overview of OIPR, how James Baker, the head of OIPR, inadvertently came to learn about Stellar Wind soon after it was initiated, and the subsequent role that OIPR played in the program's operation. We also describe the circumstances surrounding the decision to have the FISA Court Presiding Judge and his successor read into the Stellar Wind program, and the Court's response to the program. ~~(TS//STLW//SI//OC/NF)~~

---

[78] Levin told us that he did not believe Yoo was read into Stellar Wind before the October 4, 2001, Presidential Authorization was signed, and we were not able to determine precisely when Yoo's read-in occurred. However, Yoo's November 2, 2001, memorandum analyzes the legality of the October 4, 2001, Authorization and the draft of the November 2, 2001, Authorization. Thus, it appears that Yoo was read into the program not later than November 2, 2001. ~~(TS//STLW//SI//OC/NF)~~

A. Overview of OIPR (U)

At the time of the implementation of the Stellar Wind program, OIPR was responsible for advising the Attorney General on matters relating to the national security activities of the United States.[79] Created shortly after enactment of the Foreign Intelligence Surveillance Act of 1978, OIPR reviewed executive orders, directives, and procedures relating to the intelligence community, and approved certain intelligence-gathering activities. OIPR also provided formal and informal legal advice to the Attorney General and U.S. intelligence agencies regarding questions of law and procedure relating to U.S. intelligence activities. In addition, OIPR advised the Attorney General and agencies such as the CIA, FBI, and Defense and State Departments concerning questions of law relating to U.S. national security activities and the legality of domestic and overseas intelligence operations. (U//~~FOUO~~)

OIPR also represented the United States before the FISA Court. OIPR was responsible for preparing and presenting applications to the FISA Court for orders authorizing electronic surveillance and physical searches by U.S. intelligence agencies for foreign intelligence purposes in investigations involving espionage and international terrorism. When evidence obtained under FISA was proposed to be used in criminal proceedings, OIPR sought the necessary authorization from the Attorney General, and in coordination with the Criminal Division and U.S. Attorney's Office prepared the motions and briefs required by the federal court whenever surveillance under FISA was challenged. (U)

The head of OIPR was referred to as the Counsel for Intelligence Policy and was supported by two Deputy Counsel and a staff of attorneys, paralegals, and administrative professionals. James Baker served as the Counsel for OIPR from May 2001 to January 2007.[80] (U)

B. OIPR Counsel Learns of Stellar Wind Program (U//~~FOUO~~)

Baker told us that while standing outside the Department one evening several weeks after the September 11 attacks, he was approached by an FBI colleague who said, "There is something spooky going on," that it appeared

---

[79] In September 2006, the Justice Department moved OIPR into the newly created National Security Division (NSD). In April 2008, NSD modified OIPR's structure and name. The new organization is called the Office of Intelligence and includes operations, oversight, and litigation sections. For purposes of this report we use the term OIPR to reflect the time period our review encompasses. (U)

[80] Baker served as Acting Counsel for OIPR from May 2001 to January 2002, and as Counsel from February 2002 until January 2007. Baker officially resigned from the Justice Department in October 2007. (U)

foreign-to-domestic collection was being conducted without a FISA order, and that some FBI personnel "were getting nervous." The FBI colleague asked Baker whether he knew anything about the activity, and Baker responded that he did not. ~~(TS//STLW//SI//OC/NF)~~

Baker said that while reviewing a FISA application several weeks after this conversation, a particular passage regarding international communications "leapt out at" him. According to Baker, the passage contained "strange, unattributed language" and information that was "not attributed in the usual way." Baker told the OIG that the information concerned connections between telephone numbers, but he could not recall if the information simply identified a link between individuals or also included the content of communications. ~~(TS//SI//NF)~~

Baker asked the OIPR attorney responsible for the application about the information in the passage, and the attorney responded that nobody at the FBI would disclose where the information had come from, only that it was part of a "special collection." Baker therefore contacted the FBI about the application. Unable to obtain any answers to his questions, Baker informed the FBI that he would not allow the application to be filed with the FISA Court. Baker said that, to the best of his recollection, he did not believe the application was filed with the Court. ~~(TS//SI//NF)~~

Soon thereafter, Baker spoke with Daniel Levin, who at that time was serving as both Counselor to the Attorney General and Chief of Staff to the FBI Director. Levin told Baker that approval from the White House was needed before he could tell Baker about the special collection. Levin told us that he successfully pressed the White House for Baker to be read into Stellar Wind. Baker stated that David Addington, counselor to Vice President Cheney, was the individual who approved his clearance into the program. ~~(TS//STLW//SI//OC/NF)~~

According to NSA records, Baker was read into Stellar Wind in January 2002.[81] He said his read in essentially consisted of Levin providing him a short briefing and a copy of Yoo's November 2, 2001, memorandum regarding the legality of the program. Baker told us that his initial reaction was that the program, and Yoo's memorandum, were flawed legally. Baker said he did not consider himself a constitutional law scholar, but was

---

[81] Baker told us that he initially was read into the program in December 2001 by Levin. Baker said he later received a more formal briefing on the program at the NSA, where he was allowed to read the Presidential Authorizations and discuss the program with NSA attorneys. This formal briefing appears to be the event that the NSA considers Baker's official read-in, which according to NSA records occurred on January 11, 2002. We used this date for purposes of calculating the number of Justice Department employees read into the program. (U//~~FOUO~~)

nevertheless surprised that while Stellar Wind was in his view "overriding a criminal statute" on the basis of the President's power as Commander in Chief, Yoo's memorandum did not even cite an important U.S. Supreme Court opinion on presidential authority during wartime, *Youngstown Sheet & Tube Co.* Baker said he believed that it is important to exercise some "humility" when dealing with national security matters because of the complexity and importance of the issues, and he therefore reserved final judgment on the memorandum until he researched the legal issues further. Yet, Baker said his initial opinion that the memorandum was flawed legally did not change over time. ~~(TS//STLW//SI//OC/NF)~~

We asked Baker whether at the time he thought the collection authorized under Stellar Wind could have been accomplished under FISA. Baker said that his thinking on this issue has evolved over time, but that he staunchly believed that "FISA works in wartime." He stated that although it is difficult to do, FISA can be made to work under the circumstances that existed following the September 11 attacks, but that it also was easy to "make FISA not work" under these circumstances.
~~(TS//STLW//SI//OC/NF)~~

Baker cited a lack of resources as the primary impediment to using the FISA process, rather than Stellar Wind, to collect foreign intelligence following the September 11 attacks. Baker said that he did not believe OIPR, as staffed in October 2001, had sufficient resources to process the volume of telephone numbers the NSA was tasking for content collection under Stellar Wind at that time. However, Baker explained that in his view FISA is "scalable" and that to some degree the statute's utility is limited by the resources allocated to OIPR.[82] ~~(TS//STLW//SI//OC/NF)~~

Baker also observed that to bring Stellar Wind's content and meta data collections fully under FISA authority would have required a different approach to the statute. Baker said that developing such an approach would have been possible only by convening a working group to examine constitutional and practical issues. Baker, one of only three people in the Justice Department read into Stellar Wind as of January 2002, said he did not have the ability or the authority to do this himself.[83] Baker stated that his belief in this approach was informed by his own experience with and participation in a small, informal group composed of U.S. Intelligence Community officials that had worked periodically since shortly before the

---

[82] Baker also observed that OIPR could have been staffed with detailees from the Department of Defense and other components within the Justice Department. (U)

[83] Baker also said that he did not have the legal resources within OIPR to "challenge" Yoo's November 2, 2001, legal analysis of the Stellar Wind program, although he believed it was flawed. ~~(TS//STLW//SI//OC/NF)~~

September 11 terrorist attacks to develop solutions to various foreign intelligence collection issues.[84] ~~(TS//STLW//SI//OC/NF)~~

C. FISA Court is Informed of Stellar Wind ~~(TS//SI//NF)~~

Baker told the OIG that sometime in the December 2001 to January 2002 time period he concluded, based on his awareness that information derived from Stellar Wind had been used to support at least one request for a FISA application, that the FISA Court also needed to be made aware of the Stellar Wind program. Baker said that the Department's counterterrorism efforts rely on good relations with the FISA Court and that candor and transparency are critical components of that relationship. According to Baker, OIPR had a policy of full disclosure with the Court that he said served the Department well when problematic issues arose. Baker also attributed the Department's record of success with FISA applications and the improved coordination between intelligence agents and prosecutors to the strong relationship that the Department had built with the Court. Baker believed it would be detrimental to this relationship if the Court learned later that information from Stellar Wind was included in FISA applications without notice to the Court. ~~(TS//STLW//SI//OC/NF)~~

Baker said he raised the issue of the FISA Court not being informed about Stellar Wind with Levin, who first responded by suggesting that the Attorney General order Baker not to disclose the program to the Court while the issue was being considered. Baker initially agreed to this approach and drafted a memorandum from Ashcroft to Baker to this effect. He said that Levin edited the document and presented it to Ashcroft, who signed it. The memorandum, dated January 17, 2002, stated that Ashcroft understood FISA Court applications would include information obtained or derived from Stellar Wind, and that these applications would seek authorizations to conduct surveillance of targets already subject to surveillance under Stellar Wind. Ashcroft's memorandum also stated that he was considering Baker's recommendation that the Department brief the FISA Court on the program. The memorandum stated further:

> In the interim, I am directing you to file applications with the Foreign Intelligence Surveillance Court without informing the court of the existence of the Stellar Wind program or any aspect thereof. I am also directing you not to brief any other

---

[84] This type of collaborative effort ultimately developed the legal theories used to transition Stellar Wind's collection activities to FISA authority. However, as we discuss in Chapter Five, while the transition was successful with respect to bulk meta data collection, the legal theory to transition Stellar Wind's content collection, while initially approved by one FISA Court judge, subsequently was rejected by a second judge. ~~(TS//STLW//SI//OC/NF)~~

individuals in the Department of Justice, including the FBI, regarding Stellar Wind without my prior authorization. ~~(TS//STLW//SI//OC/NF)~~

Levin told us that he, as well as Ashcroft, soon came to agree with Baker that the FISA Court should be made aware of the program. Levin said he told Ashcroft during this time that Baker had done a "remarkable job" building a relationship with the FISA Court that greatly benefited the Department's counterintelligence and counterterrorism efforts. Levin said he advised Ashcroft, "We should do what Baker thinks is right." According to Levin, Ashcroft agreed. ~~(TS//STLW//SI//OC/NF)~~

Levin said that he informed Gonzales and Addington at some point of Baker's position that the FISA Court should be made aware of Stellar Wind, but said they initially rejected the idea of reading any judges into the program. Levin stated that he continued to press the issue without success. ~~(TS//STLW//SI//OC/NF)~~

However, the issue came to a head on a weekend in January 2002 when Baker reviewed a second FISA application that contained the "strange, unattributed language" Baker understood to indicate that the information referenced was obtained from the Stellar Wind program. This second FISA application sought emergency approval from the FISA Court to conduct electronic surveillance of [redacted] Because this would be the first application seeking FISA authority to monitor this particular subject's telephone communications, Baker recognized that the NSA had already engaged in some level of electronic surveillance in the United States of a domestic telephone number without a FISA order. ~~(TS//STLW//SI//OC/NF)~~

Although Baker viewed the memorandum from Ashcroft directing him not to inform the FISA Court about Stellar Wind as "cover" for him not to inform the FISA Court about Stellar Wind, he remained uncomfortable about filing an application that contained Stellar Wind information without informing the FISA Court. Baker therefore approached the Chief of the Justice Department's Professional Responsibility Advisory Office (PRAO) to discuss his ethical responsibilities to the FISA Court under circumstances where a FISA application contains certain information that is material to the Court's decision, but Baker was not authorized to disclose the source of the

information.[85] Baker stated that the PRAO Chief told him that he had an affirmative duty of candor to the Court, and that this duty of candor was heightened due to the *ex parte* nature of the FISA proceedings.[86] Baker concurred with this guidance, which Baker felt also was compelled by his position as a federal officer and officer of the Court. Baker said he therefore concluded, and informed Levin, that he would not sign the pending application or present to it to the FISA Court, nor would he allow any OIPR attorney do so. According to Baker, Levin spoke to David Addington about the situation, but Addington nevertheless declared that the Court would not be read into the program. ~~(TS//STLW//SI//OC/NF)~~

According to Baker, the White House, the Attorney General, and Levin then decided that Levin, rather than Baker, would sign the FISA application and present it to Judge Claude M. Hilton, the FISA Court judge responsible for hearing FISA matters that weekend.[87] Baker told us that he notified Judge Hilton in advance that the application was being handled in this manner. Levin said he brought the application to Judge Hilton's residence and explained that he, instead of the OIPR Counsel, was presenting the case because it involved a "special classified program." Levin told us that Judge Hilton approved the application without asking any questions. According to Levin, when he later told Addington how the matter was resolved, and that he agreed with Baker's position that the Court should be briefed into the program, Addington responded that Baker should be fired for insubordination for not signing the application. ~~(TS//STLW//SI//OC/NF)~~

According to Baker, a consensus formed after this episode among the Attorney General, the FBI, and the White House that future FISA matters could not be handled in the same fashion, particularly in view of the anticipated increase in FISA applications resulting from the intelligence collected and disseminated under Stellar Wind.[88] Baker said that the

---

[85] The Professional Responsibility Advisory Office provides advice to Department attorneys with respect to professional responsibility issues. (U)

[86] Baker cited Rule 3.3 of the American Bar Association's Model Rules of Professional Conduct as the specific rule implicated by the situation. That rule provides, in relevant part, that "in an ex parte proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer which will enable the tribunal to make an informed decision, whether or not the facts are adverse." Baker stated that he also consulted with two officials from the Office of the Deputy Attorney General on the matter and that they provided the same advice as PRAO. (U)

[87] Director Mueller and Attorney General Ashcroft already had signed the application. (U)

[88] We asked Baker whether he thought the FBI's restrictions on the use of Stellar Wind-derived leads disseminated to field offices, as described above, were sufficient to guard against including Stellar Wind information in FISA applications. Baker stated that his experience with FBI record-keeping practices did not give him a high degree of

(Cont'd.)

decision was therefore made to brief the FISA Court's Presiding Judge, Royce Lamberth.[89] ~~(TS//STLW//SI//OC/NF)~~

Judge Lamberth was read into Stellar Wind on January 31, 2002. The briefing was conducted in the Attorney General's office at the Department, and was attended by Ashcroft, Hayden, Mueller, Levin, Yoo, and Baker. According to a memorandum of talking points prepared for the briefing, Ashcroft provided Judge Lamberth a brief summary of the program's creation, explaining that the President had authorized a sensitive collection technique in response to the September 11 attacks in order to obtain foreign intelligence information necessary to protect the United States from future attacks and acts of international terrorism. Ashcroft said the NSA, at the instruction of the Secretary of Defense, implemented the collection, which was code named Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

According to the talking points, Ashcroft also discussed the factors the President considered in determining that an "extraordinary emergency exists" to support electronic surveillance without a warrant. The factors cited to Judge Lamberth paralleled those contained in the Presidential Authorizations, including "the magnitude and probability of death from terrorist attacks, the need to detect and prevent such attacks with secrecy, the possible intrusion into the privacy of American citizens, the absence of a more narrowly-tailored means to obtain the information, and the reasonableness of such intrusion in light of the magnitude of the potential threat of such terrorist acts and the probability of their occurrence." ~~(TS//STLW//SI//OC/NF)~~

According to the talking points, Ashcroft stated that he determined, based upon the advice of the Office of Legal Counsel, that the President's actions were lawful under the Constitution. Levin told us that Ashcroft emphasized to Judge Lamberth that the FISA Court was not being asked to approve the program. ~~(TS//STLW//SI//OC/NF)~~

Following Ashcroft's summary, the briefing continued in three parts. First, Hayden described how the program worked operationally. Second, Yoo discussed legal aspects of the program. Third, Baker discussed a

---

confidence that such separation could be consistently maintained. In addition, Baker believed that the nature of FBI international terrorism investigations would make it difficult to track Stellar Wind-derived information. According the FBI OGC, Baker did not share with the FBI his concerns about whether its record-keeping practices would keep Stellar Wind information from being used in FISA applications. ~~(TS//STLW//SI//OC/NF)~~

[89] The Presiding Judge for the FISA Court is appointed to a 7-year term by the Chief Justice of the Supreme Court of the United States. Judge Lamberth was appointed as Presiding Judge in 1995. (U)

proposal for handling FISA applications that contained program-derived information. ~~(TS//STLW//SI//OC/NF)~~

Levin told us that when the briefing concluded, Lamberth acknowledged he was not being asked to approve the program and expressed his appreciation for being read in. According to Baker, Lamberth also remarked, "Well, it all depends on whether you can get five votes on the Supreme Court, but I'm comfortable with it." For the next 4 months, until the end of his term in May 2002, Judge Lamberth was the only FISA Court judge read into Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

D. OIPR Implements "Scrubbing" Procedures for Stellar Wind Information in International Terrorism FISA Applications ~~(TS//STLW//SI//OC/NF)~~

Following Judge Lamberth's read-in to the Stellar Wind program, Baker implemented procedures in OIPR to address two scenarios in which Stellar Wind could affect international terrorism FISA applications.[90] First, information obtained or derived from Stellar Wind might be included in a FISA application to establish probable cause that the target of the application is a foreign power or an agent of a foreign power and that the target is using or is about to use a particular "facility" (a term used in FISA generally to refer to a specific telephone number or e-mail address) at which the electronic surveillance is directed. Second, a FISA application might target facilities that were also targeted by Stellar Wind, a situation referred to as "dual coverage" because the targeted communications were collected under two separate authorities. Baker's procedures, referred to as "scrubbing" procedures, applied to initial FISA applications as well as to renewal applications seeking to continue existing coverage of targets (electronic surveillance under FISA generally is authorized for 90-day periods). ~~(TS//STLW//SI//OC/NF)~~

Judge Lamberth required that all applications that contained NSA information derived from Stellar Wind or that would produce dual coverage of a facility be filed with him only. Baker told the OIG that the scrubbing process was his idea, with Judge Lamberth's full concurrence, and that it had as its core principle OIPR's obligation to inform the Court of all material facts contained in a FISA application. According to Baker, the scrubbing

---

[90] The procedures implemented by Baker only applied to international terrorism FISA applications, not to counterintelligence FISA applications. As Baker later explained in a letter to Judge Lamberth's successor as FISA Presiding Judge, this limitation was based on the understanding that the Stellar Wind program targeted only certain international terrorist communications "and there is no reason to believe that the fruits of Stellar Wind collection would appear in a counterintelligence FISA application." ~~(TS//STLW//SI//OC/NF)~~

procedures were a means of implementing his ethical duty of candor to the Court without disclosing the existence of the Stellar Wind program to uncleared attorneys and judges. Baker also said that Judge Lamberth wanted to be informed of applications that contained Stellar Wind information and of dual coverage situations, and that Judge Lamberth believed that the procedures devised by Baker were an appropriate and acceptable means of accomplishing this. According to Baker, the scrubbing process made him and Judge Lamberth "comfortable the Court was being told what it needed to be told."[91] ~~(TS//STLW//SI//OC/NF)~~

We describe below the initial two scrubbing procedures implemented by Baker as well as the difficulties they created for the FISA application process. ~~(TS//STLW//SI//OC/NF)~~

1. Initial Scrubbing Procedures ~~(TS//SI//NF)~~

Each international terrorism FISA application was "scrubbed" for Stellar Wind information and dual coverage before it was filed. However, Baker, as the only person in OIPR read into Stellar Wind, was unable to explain to his staff why the scrubbing was being conducted. With the NSA's cooperation, Baker initially scrubbed the applications without any assistance from OIPR staff. Baker said the time and effort he expended on this practice was not sustainable, and within weeks of beginning the scrubbing procedures Baker enlisted the assistance of OIPR's Acting Deputy Counsel for Intelligence Operations, Peggy Skelly-Nolen. Skelly-Nolen stated to the OIG that Baker told her at that time that he "needed to tell me something that he couldn't tell me," but was able to convey that he needed her and the office's assistance to process international terrorism FISA applications because the supporting declarations contained information that required special handling. ~~(TS//STLW//SI//OC/NF)~~

The scrubbing process, or "the program check" as it came to be known within OIPR, had two purposes. The first purpose was to identify draft applications that contained Stellar Wind-derived information in support of probable cause to believe that the target of the application was a foreign power or an agent of a foreign power and was using or was about to use a particular facility. The second purpose was to identify applications that targeted facilities that were already actively targeted under the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

---

[91] The FBI OGC told us that Baker never disclosed to it that the FISA Court was concerned about risks presented by the inclusion of Stellar Wind information in FISA applications, nor did Baker inform the FBI that OIPR implemented procedures to address these concerns. ~~(TS//STLW//SI//OC/NF)~~

To accomplish the first purpose, OIPR attorneys were required to identify any information in applications attributed to the NSA, even if there was no suggestion the information was derived from a special program. The OIPR attorneys provided by e-mail the relevant excerpts from the applications to a designated OIPR legal assistant, who in turn compiled the information and transmitted it to the NSA by secure e-mail or facsimile. Upon receipt, the NSA conducted a check of the identified information against the Stellar Wind reports database, among others, to determine whether the information was derived or obtained from the program (as distinguished from being obtained by some other NSA signals collection activity). The NSA provided OIPR the results of its search by return e-mail or facsimile, writing next to each excerpt either "yes" or "no" to indicate whether the information was Stellar Wind-derived. Judge Lamberth did not require that Stellar Wind-derived information be removed from FISA applications, only that any such applications be filed with him exclusively and the Stellar Wind information identified to him orally.[92]
~~(TS//STLW//SI//OC/NF)~~

The second purpose of the scrub – to identify dual collection applications – followed similar steps. On approximately a weekly basis, an OIPR legal assistant requested that OIPR attorneys transmit to him all facilities targeted for electronic surveillance in applications scheduled to be filed with the FISA Court that week. The legal assistant created a single list of all targeted telephone numbers and e-mail accounts and e-mailed or faxed the information to the NSA. The NSA in turn checked the Stellar Wind database to determine whether any of the listed facilities were tasked for content collection under the program. The NSA provided OIPR the results of this check by return e-mail or facsimile, writing next to each facility either "yes" or "no" to indicate whether the facility was tasked under Stellar Wind.
~~(TS//STLW//SI//OC/NF)~~

Baker proposed to Judge Lamberth that OIPR notify him of dual coverage cases by including in the applications a [redacted]

[redacted]

[92] Baker said that only [redacted] international terrorism FISA applications presented to Judge Lamberth included Stellar Wind information to support the application.
~~(TS//STLW//SI//OC/NF)~~

[redacted]

(Cont'd.)

[redacted] Baker proposed to include this descriptive phrase in applications that, if approved, would result in dual coverage. ~~(TS//STLW//SI//OC/NF)~~

Beginning in early 2002, any FISA applications that included the descriptive phrase [redacted] were to be presented to Judge Lamberth, [redacted] also would inform Judge Lamberth directly that it was a "Lamberth only" case to indicate it was connected to Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

2. Complications with Scrubbing Procedures ~~(TS//SI//NF)~~

Skelly-Nolen told us that no one in OIPR, including her at that time, was aware that the checks Baker was requiring the office to make concerned a specific compartmented program. However, the scrubbing procedures generated questions from OIPR attorneys and FBI agents, particularly when Skelly-Nolen instructed an OIPR attorney to add to an application the descriptive phrase [redacted] Skelly-Nolen told us that she was not able to provide a satisfactory response to the questions because she did not have the answers. ~~(TS//SI//NF)~~

Skelly-Nolen also stated that it was stressful to comply with the procedures, due in large part to the fact that the attorneys and agents responsible for the contents of the international terrorism applications were asked to follow certain procedures for filings but were not being provided an explanation for these measures. She said this stress was compounded by the concurrent anthrax scare and the prevailing belief that there would be another terrorist attack. Skelly-Nolen stated that OIPR staff was acting based on Baker's representations alone, and while Baker sought to assuage any concerns the OIPR attorneys had over these new procedures by

[redacted]

explaining to the office that he had spoken to the Attorney General and the FISA Court on the issue, some OIPR attorneys simply were not comfortable under these circumstances and Skelly-Nolen had to reassign the international terrorism cases these attorneys were handling. Baker stated that he regularly told attorneys that they did not have to sign applications that they were not comfortable with. ~~(TS//SI//NF)~~

The process for filing international terrorism FISA applications was further complicated by the fact that of the two Justice Department officials authorized to approve such applications – the Attorney General and the Deputy Attorney General – only Attorney General Ashcroft was read into Stellar Wind.[94] As mentioned previously, Larry Thompson, who served as Deputy Attorney General from May 2001 to August 2003, was never read into the Stellar Wind program. Alberto Gonzales, who served as White House Counsel from January 2000 to February 2005, stated to the OIG that he recalled that Ashcroft wanted Thompson, as well as Ashcroft's Chief of Staff, read into Stellar Wind, but that neither official ever was. Gonzales said Ashcroft complained that it was "inconvenient" not having these two officials read into the program.[95] ~~(TS//STLW//SI//OC/NF)~~

The situation with Thompson caused Associate Deputy Attorney General David Kris, who oversaw national security matters in the Office of the Deputy Attorney General during Thompson's tenure, to draft a memorandum on January 11, 2002, advising Baker that he should not send Kris any FISA applications that included information obtained or derived from the Stellar Wind program, and that Kris intended to advise Thompson not to review or approve any such applications.[96] The memorandum stated that Kris was aware of the existence of a "highly classified information-collection program that has the unclassified code name 'Stellar Wind'," but that he was "wholly unaware of the nature and scope of the

---

[94] Each FISA application must be approved by the Attorney General, defined under § 1801(g) to include the Deputy Attorney General or Acting Attorney General, based on the Attorney General's finding that the application "satisfies the criteria and requirements of such application as set forth in [subchapter I concerning electronic surveillance]." 50 U.S.C. § 1804(a). (U)

[95] As noted above, Gonzales also told the OIG that he never got the sense from Ashcroft that the situation affected the quality of the legal advice the Department provided to the White House. However, as described in Chapter Four, others had a decidedly different impression of Ashcroft's opinion of the legal advice he received on Stellar Wind during this period. We were unable to interview Ashcroft about this issue. ~~(TS//SI//NF)~~

[96] Baker told the OIG that he had informed Kris about the existence of a classified program that he could not discuss further, and that it impacted FISA applications. Baker said he and Kris agreed that, under the circumstances, it was not appropriate for Thompson to sign applications if he was not fully informed about all of the material facts related to them. ~~(TS//SI//NF)~~

program." Kris also stated in the memorandum that his request for a briefing on the program had been denied and that he was aware Deputy Attorney General Thompson also had not been briefed on the program.[97] ~~(TS//STLW//SI//OC/NF)~~

E. Judge Kollar-Kotelly Succeeds Judge Lamberth as FISA Court Presiding Judge (U)

Judge Lamberth's 7-year term on the FISA Court ended in May 2002. On May 19, 2002, Judge Colleen Kollar-Kotelly was appointed to the Court to replace Lamberth as the Presiding Judge. In connection with this appointment, Judge Kollar-Kotelly was read into the Stellar Wind program and provided an opportunity to examine the Department's analysis of the program's legality. Judge Kollar-Kotelly also spoke with Baker on numerous occasions about the scrubbing procedures he implemented to account for Stellar Wind information in international terrorism FISA applications and to identify applications that would result in dual coverage. ~~(TS//STLW//SI//OC/NF)~~

1. Judge Kollar-Kotelly Modifies OIPR Scrubbing Procedures ~~(TS//SI//NF)~~

Judge Kollar-Kotelly received her first briefing on the Stellar Wind program in the Attorney General's office on May 17, 2002, 2 days prior to being formally appointed Presiding Judge for the FISA Court. Baker, who attended the briefing, told us that the presentation was similar to the briefing initially provided to Judge Lamberth. Judge Kollar-Kotelly had several questions concerning the scope of the President's authority to conduct warrantless surveillance, and the Department responded that same day with a letter signed by OLC Deputy Assistant Attorney General Yoo that outlined the legal basis for the activity. The letter essentially replicated Yoo's November 2, 2001, memorandum regarding the legality of Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

According to Baker, Judge Kollar-Kotelly met at the White House with Addington, Gonzales, and Yoo to read Yoo's letter, but she was not permitted to retain a copy or take any notes. Judge Kollar-Kotelly later wrote in a letter to Baker that Yoo's letter "set out a broad overview of the legal authority for conducting [Stellar Wind], but did not analyze the specifics of the [Stellar Wind] program." ~~(TS//SI//NF)~~

---

97 [redacted]

~~(TS//SI//NF)~~

Judge Kollar-Kotelly also requested an opportunity to review the Presidential Authorization initiating Stellar Wind. On August 12, 2002, she reviewed the October 4, 2001, Authorization. ~~(TS//SI//NF)~~

Baker said that he met with Judge Kollar-Kotelly on several occasions after her initial Stellar Wind briefing to discuss how OIPR had been handling Stellar Wind's impact on FISA applications. Baker described for her the existing procedures to account for NSA information contained in FISA applications derived from Stellar Wind, and to identify applications that, if approved, would produce dual coverage of a facility. ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly also was interested in identifying whether a facility targeted in a FISA application had been tipped to the FBI as Stellar-Wind derived information. Baker told the OIG that at this time he did not believe the FBI and NSA had the ability to track Stellar Wind tips on a timely basis. Baker said he mistakenly believed that as tips passed from the NSA to FBI Headquarters, and from there to FBI field offices for investigation, it would be exceedingly difficult to trace the specific source of the information in a sufficiently timely manner for inclusion in a FISA application. Baker provided his understanding to Judge Kollar-Kotelly, likening the Stellar Wind information in tips to the FBI as "salt in soup" that is impossible to extract once added. Based on Baker's representations, Judge Kollar-Kotelly did not require the Department to identify whether a facility targeted in a FISA application was ever provided to the FBI under Stellar Wind.[98] ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly decided that the scrubbing procedures implemented under Judge Lamberth should continue, but she directed OIPR to discontinue including in applications the descriptive phrase [redacted] as a means of notifying her that facilities targeted by the applications were also targeted under Stellar Wind. Baker said that while Judge Kollar-Kotelly understood that instances of dual coverage would occur, she did not want to appear to judicially sanction Stellar Wind coverage. Baker told us his impression was that Judge Kollar-Kotelly "did not want to rule on the legality of the program" by appearing to "authorize" the NSA's technique for collecting the same information the government was seeking to collect under FISA.[99]

---

[98] Baker eventually learned that the FBI and the NSA in fact did have some ability to track Stellar Wind information. As discussed in Chapter Six, in March 2004 Judge Kollar-Kotelly added to the scrubbing process a check performed by the FBI to determine whether any telephone numbers or e-mail addresses contained in a FISA application had ever been provided to the FBI in a Stellar Wind report. ~~(TS//STLW//SI//OC/NF)~~

[99] Judge Kollar-Kotelly later wrote about the dual coverage issue, in a January 12, 2005, letter to Baker that discussed the "Stellar Wind Program and Practice Before the (Cont'd.)

Baker said he believes Judge Kollar-Kotelly was trying to protect the FISA Court and did not want the legality of the Court's orders called into question. ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly also directed OIPR to excise from FISA applications any information obtained or derived from Stellar Wind. Baker told Judge Kollar-Kotelly that OIPR could implement this requirement using the scrubbing procedures already in place, and that where the FBI included NSA information in an application determined to be Stellar Wind-derived, OIPR would excise it. ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly also instructed Baker to alert her of any instances where an application's basis for the requisite probable cause showing under FISA was weakened by excising the Stellar Wind information. In such cases, Judge Kollar-Kotelly would then decide whether to approve the application with the knowledge that additional relevant information had been excised. ~~(TS//STLW//SI//OC/NF)~~

Even though Judge Kollar-Kotelly's scrubbing process was intended to eliminate all Stellar Wind information from international terrorism FISA applications, she still required that scrubbed applications be filed with her only. In time, Judge Kollar-Kotelly relaxed this requirement and permitted other judges on the Court to handle these applications, although only after first being filed with her.[100] ~~(TS//STLW//SI//OC/NF)~~

2. OIPR implements Judge Kollar-Kotelly's Scrubbing Procedure ~~(TS//SI//NF)~~

According to Baker and Skelly-Nolen, the mechanics within OIPR for determining whether an application contained Stellar Wind information or targeted a facility also targeted under Stellar Wind remained essentially unchanged after the transition from Judge Lamberth to Judge Kollar-Kotelly. However, the scrubbing process became more complex. For

---

FISC." The letter memorialized the information Judge Kollar-Kotelly received from the government about the program and how she requested the government to proceed in preparing and presenting applications. On the subject of dual coverage, Judge Kollar-Kotelly wrote, "Without opining on [Stellar Wind]-related legal issues, I have sought to protect the proper functioning of the FISA process, under which separate court authorities are granted to conduct foreign intelligence collection against a set of targets that overlaps the set of [Stellar Wind] targets." We discuss this letter in Chapter Four of this report. ~~(TS//STLW//SI//OC/NF)~~

100 [redacted]

example, because only the Attorney General could sign the applications and Judge Kollar-Kotelly required that only she receive the applications (even after being scrubbed), Skelly-Nolen had to regularly visit the Attorney General's and Presiding Judge's residences with stacks of what Skelly-Nolen came to refer to as "AG-KK only" FISA applications. ~~(TS//STLW//SI//OC/NF)~~

The situation was further complicated when Ashcroft was on overseas travel and his signature was needed for a scrubbed application ready to be filed. When this occurred, the classification of the application's signature page was "downgraded" and then sent to Ashcroft by secure fax. The actual application was not faxed; instead, Skelly-Nolen typically included a statement from her or Baker with the signature page indicating that the application was proper and complied with the requirements of the FISA statute. Skelly-Nolen observed that in these cases Ashcroft essentially relied on her and Baker's assessments of the applications – even though Skelly-Nolen was not read into Stellar Wind at this time. Scrubbed applications were handled similarly when Ashcroft was traveling domestically, although in those instances the applications could be provided along with the signature page if requested.[101] ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly also required that hearings for the "AG-KK only" FISA applications and renewals be scheduled for late in the day or on the weekend, either in her courtroom chambers at the District Court for the District of Columbia or at her residence. According to Skelly-Nolen, Judge Kollar-Kotelly insisted on this practice so that the "AG-KK only" docket did not interfere with her regular court docket. From Skelly-Nolen's perspective, this practice proved to be an "enormous burden," particularly in cases involving applications to continue FISA coverage on targets of emergency authorizations.[102] Skelly-Nolen explained that these authorizations were, for "no good operations reason" that she was aware of, routinely approved by the Attorney General on Fridays, meaning that a FISA application had to be filed with the Court within 72 hours – by Monday – to continue the emergency surveillance coverage. However, because Judge Kollar-Kotelly had a regular court docket on Mondays, she required that any scrubbed FISA application seeking authority to continue surveillance initiated under

---

[101] Baker and Skelly-Nolen told the OIG that in their experience it was not unusual for an Attorney General or Deputy Attorney General to rely on OIPR's representations that the FISA applications presented for signature satisfied the statute's requirements, instead of reviewing the full contents of each application. (U//~~FOUO~~)

[102] As previously described, under FISA during this time period, when the Attorney General reasonably determines that an emergency situation exists prior to obtaining a FISA order, the Attorney General may approve the use of electronic surveillance for a period of up to 72 hours without an order. (U)

emergency authorization be scheduled with her for Sunday. Skelly-Nolen stated that these cases would be in addition to the renewal applications that also had to be heard on Sundays so the authority for the surveillance in those cases did not expire and the coverage lapse.
~~(TS//STLW//SI//OC/NF)~~

Baker identified another issue that stemmed from Judge Kollar-Kotelly's requirement that only she receive dual coverage applications. The problem arose when Judge Kollar-Kotelly was out of town and unavailable to hear a dual coverage application. Baker's solution was either to fly the application to the place Judge Kollar-Kotelly was located, or to contact the NSA and request that it "de-task" the facilities that the FISA application was targeting. In this way, the application could be presented to an alternative FISA Court judge because it no longer targeted facilities that were also targeted under Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

For example, Baker described a situation where the FBI was urgently interested in a particular individual whose telephone was currently tasked by the NSA under Stellar Wind. In this case, Baker instructed the NSA to de-task the telephone number so the FBI's FISA application could be presented to a judge other than Judge Kollar-Kotelly. To prevent any gap in coverage between the time the NSA detasked the telephone number and the Court approved the FBI's application, surveillance was initiated under FISA's emergency authorization provision and then presented to a FISA Court judge within the requisite 72 hours. According to Baker, proceeding in this fashion "made everyone comfortable," including the NSA. Baker told us that this situation occurred a couple of times each year.
~~(TS//STLW//SI//OC/NF)~~

According to Baker and Skelly-Nolen, these examples illustrate how having only the Attorney General and a single judge on the FISA Court read into Stellar Wind complicated the FISA process. Baker said that "fairly early on" after being read into the program, Judge Kollar-Kotelly made several requests for other FISA Court judges to be read into the program. Baker told the OIG that these requests were generally made through him, orally and in writing, but was aware that on at least one occasion Judge Kollar-Kotelly made the request directly to Attorney General Ashcroft. Baker said that sometime prior to March 2004 he personally advised Ashcroft of Judge Kollar-Kotelly's concerns, and that Ashcroft responded with words to the effect that the White House would not allow more judges to be read into Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

In a January 12, 2005, letter to Baker, Judge Kollar-Kotelly summarized the situation, stating, "I have repeatedly asked that the other members of the FISC be given access to the same information that I have received regarding the [Stellar Wind] program. To date, the executive

branch has declined to do so, citing a need to maintain the strictest secrecy regarding [Stellar Wind]." ~~(TS//STLW//SI//OC/NF)~~

As a consequence of only Judge Kollar-Kotelly being read into Stellar Wind and her insistence that she alone handle applications scrubbed of Stellar Wind information or that involved tasking telephone numbers or e-mail addresses already tasked under Stellar Wind (dual coverage), by November 2004 she was handling approximately [redacted] percent of all FISA applications. Judge Kollar-Kotelly also tended to hear successive applications regarding the same targeted facilities. She discontinued this practice in November 2004 and permitted other judges to hear scrubbed applications. Judge Kollar-Kotelly later wrote that her decision was "based on the operational systems" OIPR had in place to scrub applications and that she assured her colleagues "that they could properly decide [the cases] based on the information in each application, without the additional information on which I have been briefed, but which, to date, the other judges have not received." ~~(TS//STLW//SI//OC/NF)~~

V. FBI Initiates Measures to Improve the Management of Stellar Wind Information ~~(S//NF)~~

Following the terrorist attacks of September 11, the FBI had reallocated personnel and resources to counterterrorism operations, and established the Telephone Analysis Unit (TAU) to exploit telephone communications data. We described above how a small team of agents and analysts from this unit was reassigned to the [redacted] which was responsible for handling the Stellar Wind reports provided by the NSA. ~~(S//NF)~~

In approximately May 2002, the TAU was renamed the Communications Analysis Unit (CAU) and became one of the units within the newly created Communications Exploitation Section (CXS). According to the first Acting CAU Unit Chief, the FBI's vision for the unit was that it would support FBI international terrorism investigations by [redacted] The Stellar Wind program was one source for obtaining this [redacted] ~~(S//NF)~~

In this section, we describe changes the FBI implemented in late 2002 and early 2003 to manage the intelligence it received under Stellar Wind. These changes included attempts to improve coordination with the NSA, implement a more formal program to receive intelligence from the NSA and disseminate it to FBI field offices, educate the FBI field offices about the value of the intelligence and FBI Headquarters' expectations concerning its use, and assign a small team of FBI personnel to work full-time at the NSA on Stellar Wind. ~~(S//NF)~~

A. CAU Acting Unit Chief Evaluates FBI Response to Stellar Wind ~~(S//NF)~~

When the first CAU Unit Chief arrived at FBI Headquarters in September 2002, CXS was newly established and most of the Section's 15-20 staff was there on temporary duty assignments. The CAU was staffed similarly at this time, but also contained some professional support employees from other divisions at FBI Headquarters. ~~(S//NF)~~

The CAU Unit Chief said that the CAU's mission was to support FBI international terrorism investigations – al Qaeda investigations in particular – by analyzing telephone calling activity and e-mail communications. He explained that prior to September 11, 2001, the FBI analyzed telephone numbers received by field offices or other sources by querying the numbers against the FBI's [redacted] database, the FBI's central repository for telephone subscriber data. However, he said the FBI's database at that time was relatively small and had limited analytical capability. In the wake of the September 11 attacks, the FBI gained access to additional tools and began to utilize more sophisticated analytical techniques. Stellar Wind was one of those new tools. ~~(TS//STLW//SI//OC/NF)~~

The CAU Unit Chief said that after he was read into Stellar Wind in late September 2002, it was clear to him based on conversations with the CXS Acting Section Chief that the FBI wanted to increase its participation in the Stellar Wind program. As a counterterrorism agent in the FBI's Chicago field office, the Unit Chief had some exposure to Stellar Wind in the form of [redacted] leads. He told us that he had recalled thinking the leads were "stupid" and "not sensible." He also said that he had been critical of the leads because they did not provide any context to the information, such as how it was obtained. He stated that the leads did not adequately explain the [redacted] rankings associated with the telephone numbers, and the leads were not sufficiently specific as to what action the field office was expected to take. In his view, the intelligence disseminated by the [redacted] ECs was not "actionable." The Unit Chief told us that he could not figure out why FBI Headquarters was "pushing this stuff out" after September 11, and that other agents in the field shared his views.[103] ~~(TS//STLW//SI//OC/NF)~~

---

[103] As previously described, former NSA Director Hayden told us that immediately following the September 11 terrorist attacks the NSA modified the agency's collection [redacted] and that this resulted in a flood of telephone numbers to the FBI. Thus, it is possible that (Cont'd.)

After becoming the acting Unit Chief for the CAU and reviewing how the FBI was handling the Stellar Wind information, he learned that there was no unit that oversaw the [redacted] and no guidance for how the NSA information should be processed by FBI analysts. He also said that the process in place – essentially re-typing into ECs the tearline information contained in Stellar Wind reports – merely "regurgitated" information that, by itself, was not actionable. He was not critical of the FBI analysts responsible for drafting the ECs, who simply performed this task as directed. Rather, he believed the process suffered from a lack of leadership. He described the FBI's involvement in Stellar Wind up to this point as "happenstance" and said the FBI did not have "a real good handle on it." He said that the deficiencies he identified were attributable in part to the significant resource challenges the FBI encountered after September 11, but he nevertheless considered the FBI's effort to respond to the Stellar Wind information as "half-baked." He said he therefore set about implementing changes within the CAU to better organize this effort, which he believed would improve the quality of the intelligence disseminated to FBI field offices. ~~(TS//STLW//SI//OC/NF)~~

B. FBI Increases Cooperation with NSA and Initiates [redacted] Project to Manage Stellar Wind Information ~~(TS//STLW//SI//OC/NF)~~

The CAU Unit Chief said that the first step he took to improve the FBI's involvement in Stellar Wind was to detail to the NSA one of CAU's temporary duty special agents. He instructed the agent to form a working group at the NSA to identify any problems and evaluate the quality of the information provided in the NSA's Stellar Wind reports, as well as the information that the FBI reported back to the NSA about tips.[104] The CAU Unit Chief said he took this step so that the NSA gained a "case agent's perspective" on the type of information useful to FBI field offices, and also to explain to the NSA that the information that could be disseminated about the tippers should include "context" and "clarity" sufficient to justify the FBI conducting an inquiry under the FBI's investigative guidelines.[105] He said he did not believe that the NSA's interest in obscuring the "sources and methods" associated with the information had to compromise the quality of the information provided to the FBI. He also said that the NSA needed to

---

FBI agents' early frustration with leads that provided telephone numbers was attributable in part to the leads generated under this NSA collection activity. ~~(TS//STLW//SI//OC/NF)~~

[104] The CAU Unit Chief recalled that the NSA had expressed frustration that the FBI never provided the NSA any responses to the tipped information. ~~(S//NF)~~

[105] FBI international terrorism investigations at this time were governed by the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations. (U)

understand how the FBI investigated intelligence that it received, and that FBI agents did not have to know the specific sources and methods used to acquire information in order to effectively investigate the information. ~~(S//NF)~~

The CAU Unit Chief said that this liaison effort occurred over a couple of weeks, with the temporary duty agent driving to the NSA daily. According to the Unit Chief, the agent explained to NSA personnel what the FBI was permitted to do with certain types of information and that the NSA would receive more feedback from the FBI if the quality of the disseminable information about the tippers improved. The Unit Chief told us that following this exchange the NSA improved the Stellar Wind reports by providing better information in both the compartmented and tearline portions of the reports. ~~(S//NF)~~

In addition, the CAU Unit Chief told us that he took steps to increase cooperation within the FBI between CAU, which was part of an analytical section that supported counterterrorism investigations, and FBI Headquarters' International Terrorism Operations Section, which was responsible for overseeing FBI counterterrorism investigations. The Unit Chief said that based on his experience in the field working counterterrorism cases, he believed it was important that the CAU analysts consult with agents in the operational section about leads the CAU proposed to set in the ECs. While he was confident the CAU analysts could identify logical investigative steps, he thought they should nevertheless coordinate with the operational personnel to see if there was agreement and to determine whether a lead potentially could affect any ongoing operations that the CAU was not aware of. He also noted that his CAU Unit Chief successors discontinued this practice, a decision he disagreed with and complained about to the Section Chief for CXS because he believed the program risked losing a measure of effectiveness and efficiency as a consequence. ~~(S//NF)~~

Another step the CAU Unit Chief took relating to the FBI's management of Stellar Wind information was to open an administrative file, or "control file," to serve as the repository for all communications that the CAU sent to the field offices containing Stellar Wind information, as well as all communications the CAU received from field offices reporting the results of the investigative activity taken in response to assigned leads.[106] As explained previously, the [redacted] communications had been

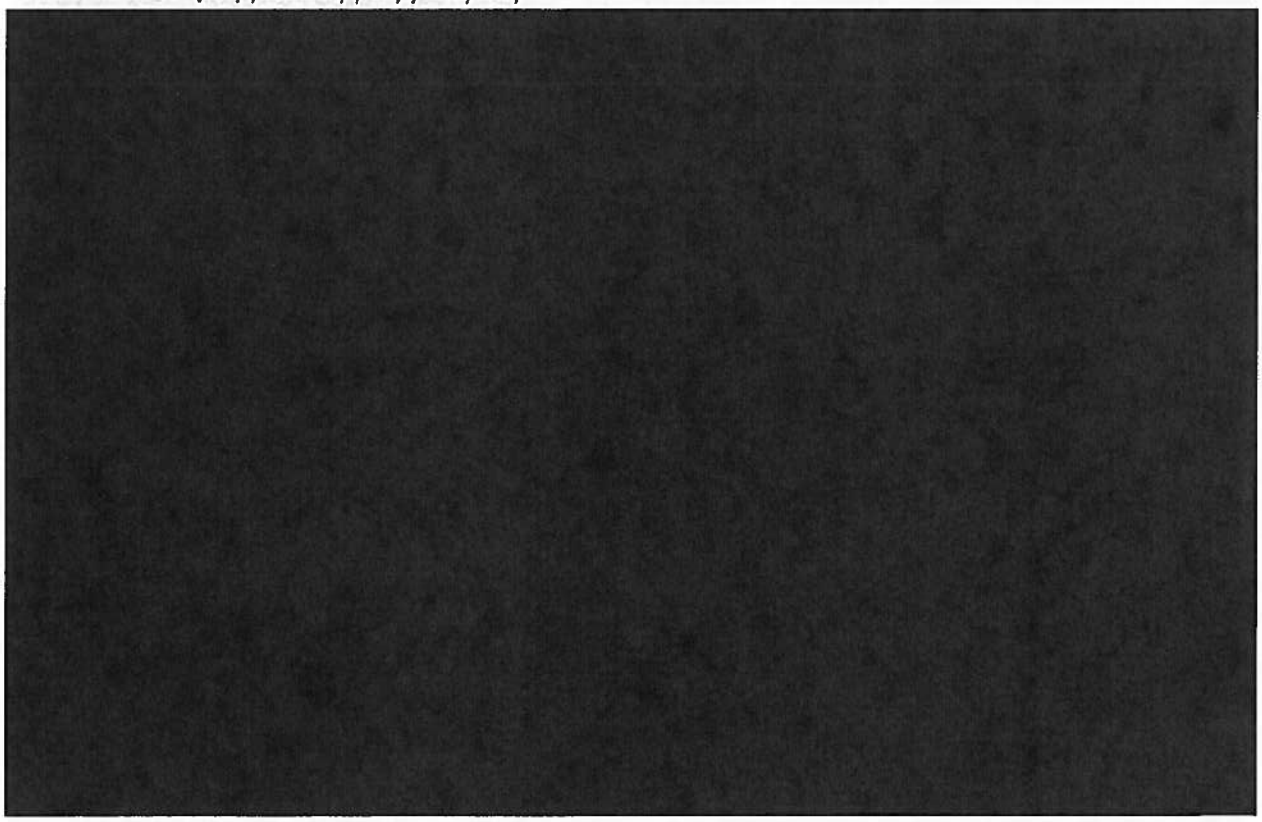
[redacted]

disseminated from a subfile associated with the FBI's international terrorism investigation of the September 11 attacks. In the EC requesting that a control file be opened for Stellar Wind information, the CAU Unit Chief wrote that "a dedicated control file for this project will better serve the specific needs of the special project and will add an additional layer of security for the source." ~~(TS//STLW//SI//OC/NF)~~

A control file for Stellar Wind information was opened on September 30, 2002, and given the designation [redacted] From that point forward, all ECs that disseminated Stellar Wind tips were sent in connection with the [redacted] control file.[107] The ECs were classified at the Secret level and, similar to the [redacted] ECs, included a vague explanation about the source of the information and a caveat concerning its use.[108] ~~(TS//STLW//SI//OC/NF)~~

---

[107] The Unit Chief told us that Director Mueller held a telephone conference call in October 2002 with the heads of all FBI field offices and advised them that FBI Headquarters was working to improve the process for disseminating [redacted] information to the field offices by adding both context and clarity to the communications. Director Mueller expressed his expectation that the offices would act on the information. According to the Unit Chief, Director Mueller essentially was trying to sell the program and ensure the "tool" was being used. Director Mueller told the OIG that he did not recall having specific discussions with the heads of FBI field offices about Stellar Wind information. ~~(TS//STLW//SI//OC/NF)~~



Several months later, in January 2003, the CAU Unit Chief sent an EC to all FBI field offices seeking "to clarify the mission of [CAU] . . . as well as to describe this unit's distinct role in the FBI's participation in the global war on terror." The EC emphasized CAU's capabilities in examining telephone calling activity and its liaison function with members of the U.S. Intelligence Community that are "in a unique position to provide potentially actionable intelligence to the FBI." The EC explained that many of the leads from the CAU were sent under the [redacted] file. On the subject of investigative responses to [redacted] leads, the EC stated:

[redacted]

C. FBI Assigns CAU Personnel to NSA on Full-Time Basis ~~(S//NF)~~

The CAU Unit Chief also assigned a team of FBI personnel to the NSA on a full-time basis to manage Stellar Wind information. The Unit Chief told us that shortly before his temporary duty assignment to FBI Headquarters was set to expire, he and the CXS Acting Section Chief briefed Director Mueller's assistant – and later Director Mueller – about the role they recommended that the FBI take in the Stellar Wind program. The CAU Unit Chief recommended co-locating at the NSA approximately four FBI agents and analysts with remote access to FBI information systems. He likened the suggestion to a "task force environment" that would introduce the FBI's investigative skills at the beginning of the NSA's analysis of Stellar Wind information. Director Mueller approved the recommendation and told the CAU Unit Chief to implement it. ~~(S//NF)~~

For the next 2 months, the CAU Unit Chief worked with the NSA on the proposal. [redacted]

[redacted] The Memorandum of Understanding between the FBI and the NSA to facilitate the co-location was finalized in December 2002, and in February 2003 a CAU team began its co-location at the NSA to manage the FBI's involvement in Stellar Wind. This co-location continues today. ~~(TS//STLW//SI//OC/NF)~~

VI. OIG Analysis (U)

In analyzing the Department's and the FBI's involvement in the NSA's expanded signals intelligence collection activity after the September 11 attacks, it is important to recognize the exceptional circumstances that existed at the time. Many Department and FBI officials emphasized to us the sense of crisis and alarm during this period, and noted the widely shared concern within the Intelligence Community that a second wave of attacks was imminent. The Stellar Wind program was conceived and implemented amid these challenging circumstances. ~~(S//NF)~~

This chapter described the role of Justice Department and FBI officials in the inception and early implementation of the Stellar Wind program, including the Department's initial reviews of the legality of the program. ~~(TS//SI//NF)~~

We believe that a significant problem during this early phase of the Stellar Wind program was the lack of a sufficient number of Justice Department attorneys read into the program to conduct an analysis of the program's legality. The White House – and according to Gonzales, the President – determined who within the Department was permitted access to the program. We believe that Attorney General Ashcroft, who met frequently with the President on national security matters, was in a position to personally advocate for the read-in of an adequate number of attorneys necessary for the Department to perform a thorough and factually accurate legal analysis of the program. We know that Ashcroft's request that his chief of staff David Ayres and Deputy Attorney General Larry Thompson be read into the program was not granted. But because Ashcroft did not agree to be interviewed, we were unable to determine from him whether he sought additional Department read-ins to assist in the legal analysis of the program, how hard he may have pressed for these additional resources, or whether he believed he was receiving adequate legal advice about the program from Yoo alone. ~~(TS//SI//NF)~~

As described in this chapter, John Yoo was the only Department attorney read in to work on the legal analysis supporting the program from

September 2001 through May 2003.[109] As described in Chapter Four, Department officials who succeeded Yoo concluded that the analysis Yoo produced was significantly flawed and found the legal basis for aspects of the program to be lacking. We believe that reading in only one Department attorney to analyze the legality of the program impeded the Department's ability to conduct a thorough and factually accurate legal analysis, and undermined the Department's early role in the program. In Chapter Four we discuss the harm that resulted in late 2003 and early 2004 from the Department's highly restricted access to the program. ~~(TS//SI//NF)~~

We also described in this chapter how the harm attributable to the Justice Department's insufficient early involvement in the program extended beyond conducting an analysis of the program's legality. The Justice Department's relationship with the FISA Court was put at risk by not having officials from OIPR and members of the FISA Court read into Stellar Wind when program-derived information started being disseminated as investigative leads to FBI field offices. In our view, it was foreseeable that Stellar Wind-derived information would be included in FISA applications.[110] OIPR Counsel Baker told us that the Department's counterterrorism and counterintelligence efforts rely on good relations with the FISA Court and that candor and transparency are critical components of the relationship. Baker attributed the Department's record of success with FISA applications and the improved coordination between intelligence agents and prosecutors to the strong relationship that the Department built with the Court. Baker believed, and we agree, that it would have been detrimental to the relationship if the Court learned that information from Stellar Wind was

---

[109] As was the case with Ashcroft, because Yoo did not agree to be interviewed we were unable to learn from him what if any efforts he made either within the Department or at the White House to advocate for additional attorneys – including his supervisor in OLC – to be read into the program to assist in his legal analysis. However, in his book "War by Other Means," Yoo wrote of his experience working on the Stellar Wind program:

> While meeting with Ashcroft alone reflected the importance of the issues, it also placed me in a difficult position. I could not discuss certain matters with my DOJ superiors, or rely on the collective resources of OLC, which usually assigned several attorneys to work on an opinion. Operational security demanded by the war on terrorism changed some of OLC's standard operating procedures.

War by Other Means at 101. ~~(S//NF)~~

[110] The restrictions the FBI imposed on the use of program-derived information – that it could be used for "lead purposes" only and not for "legal or judicial purposes" (such as affidavits) – reflected a good faith and reasonable effort. However, such restrictions could not ensure that program-derived information would not appear in FISA applications. Indeed, this eventuality led to Baker's discovery of the program. ~~(TS//STLW//SI//OC/NF)~~

included in FISA applications without the Court being told so in advance. ~~(TS//STLW//SI//OC/NF)~~

Yet we are not aware of any effort or consideration on the part of Attorney General Ashcroft or officials at the White House to account for Stellar Wind's impact on Justice Department FISA operations by reading in any OIPR officials or members of the FISA Court. In fact, as we described in this chapter, Baker was read into Stellar Wind only after hearing from an FBI colleague that "there is something spooky going on" with the collection of foreign-to-U.S. communications and subsequently reviewing a FISA application that contained "strange, unattributed" language that the FBI would not explain to him. Baker was read in when Daniel Levin, then Counselor to Ashcroft and Chief of Staff to Mueller, pressed White House officials for the clearance. ~~(TS//STLW//SI//OC/NF)~~

Moreover, White House officials initially rejected the idea of reading in members of the FISA Court, and then took no action even as Levin, who together with Ashcroft agreed with Baker that the Court needed to be informed about the program, continued to press the issue. It was not until Levin was required to sign and file a FISA application that Baker refused to handle because it contained Stellar Wind-derived information that the decision was made to read in a single judge (Presiding Judge Lamberth, followed by Presiding Judge Kollar-Kotelly). ~~(TS//STLW//SI//OC/NF)~~

The decisions to read in Baker and a member of the FISA Court, which in our view were unnecessarily delayed, were important steps in preserving the relationship the Justice Department had built with the Court. However, we believe that once Stellar Wind's impact on the Justice Department's FISA operations became evident, limiting read-ins to a single OIPR official and a single FISA Court judge was unduly restrictive and short-sighted. This chapter described how the scrubbing procedures imposed by the FISA Court and implemented by OIPR to account for Stellar Wind-derived information created concerns among some OIPR attorneys about the unexplained changes being made to their FISA applications. The scrubbing procedures also substantially distorted the assignment of cases to FISA Court judges and by November 2004 resulted in Judge Kollar-Kotelly handling approximately [redacted] percent of all FISA applications. In our view, once Stellar Wind began to affect the functioning of the FISA process, OIPR and the FISA Court effectively became part of the program's operations and the number of OIPR staff and FISA Court judges read into Stellar Wind to manage the impact should have increased. ~~(TS//STLW//SI//OC/NF)~~

This chapter also described the FBI's handling of Stellar Wind-derived information in the initial weeks and months of the program. The FBI's chief objective during this period was to expeditiously disseminate

program-derived information to FBI field offices for investigation while protecting the source of the information and the method by which it was obtained. We concluded that the FBI's procedures to meet this objective generally were reasonable. The FBI personnel assigned to the [redacted] developed a straightforward process for receiving Stellar Wind reports, reproducing the information in a non-compartmented, Secret-level format, and disseminating the information in Electronic Communications, or ECs, to the appropriate field offices for investigation. The [redacted] ECs disseminated to FBI field offices also placed appropriate restrictions on how the information could be used, instructing field offices that the information was "for lead purposes only" and could not be used for any legal or judicial purpose. FBI personnel at the field offices we visited as part of our review generally were familiar with the restrictions. ~~(S//NF)~~

However, we found that the exceptionally compartmented nature of Stellar Wind created deficiencies in the FBI's initial process for handling program-derived information and understandably frustrated agents assigned to handle [redacted] leads. The limited resources allocated to the [redacted] hampered the analysts' ability to enhance Stellar Wind information with relevant FBI or public source information before disseminating leads to field offices for investigation. More significantly, the [redacted] was prohibited from disclosing information that agents traditionally were accustomed to receiving with leads that required investigation. The [redacted] ECs consequently suffered from vagueness about the source of the information being provided and lacked factual details about the individuals allegedly involved with international terrorism and with whom the domestic numbers being disseminated possibly were in contact. ~~(S//NF)~~

We found that the FBI sought over time to address these deficiencies and improve the effectiveness of its participation in the Stellar Wind program. In April 2002, transmitting Stellar Wind-derived leads to FBI field offices became a priority of the Communications Exploitation Section, and within it, the Communications Analysis Unit (CAU). The first chief of the CAU assigned a team of FBI personnel to work full-time at the NSA on Stellar Wind and to initiate the [redacted] project to manage the FBI's participation in Stellar Wind. As we discuss in this chapter and in Chapter Six, these measures enhanced the FBI's knowledge about Stellar Wind operations and gave the NSA better insight about how FBI field offices investigated Stellar Wind information, which improved Stellar Wind reports and the leads that were disseminated to FBI field offices. ~~(TS//STLW//SI//OC/NF)~~

CHAPTER FOUR
LEGAL REASSESSMENT OF STELLAR WIND (MAY 2003 THROUGH MAY 2004) ~~(TS//SI//NF)~~

By early 2003, while the operation of the Stellar Wind program had evolved, particularly with respect to the means by which intelligence from the program was provided to the FBI, the program still remained legally premised on John Yoo's November 2001 and October 2002 Office of Legal Counsel memoranda. ~~(TS//SI//NF)~~

This chapter describes the pivotal period between May 2003 and May 2004 during which Yoo's departure from the Office of Legal Counsel and the arrival of new officials at the Justice Department resulted in a comprehensive reassessment of the Stellar Wind program's legal basis. This legal reassessment led to a contentious dispute between the Justice Department and the White House on the legality of important aspects of the program. This dispute eventually resulted in modifications to the operation of the program, and also contributed to the decision to place at least one aspect of the program under FISA authority. ~~(TS//STLW//SI//OC/NF)~~

Section I of this chapter discusses how personnel changes within the Office of Legal Counsel led to a re-examination of Yoo's legal analysis, culminating in a Justice Department legal position against continuing to certify the program and the resulting dispute with the White House. Section II describes how, faced with the prospect that the Attorney General, Deputy Attorney General, FBI Director, and other senior Department officials would resign in March 2004 if the program continued unchanged, the White House agreed to modify the program to conform it to the Department's revised legal analysis. ~~(TS//SI//NF)~~

I. Justice Department Reassesses Legality of Stellar Wind Program ~~(TS//SI//NF)~~

A. Overview of Office of Legal Counsel (U)

One of the responsibilities of the Assistant Attorney General for the Office of Legal Counsel (OLC) is to assist the Attorney General in his function as legal advisor to the President and all Executive Branch agencies. OLC drafts legal opinions for the Attorney General and also provides its own opinions in response to requests from the Counsel to the President, various agencies of the Executive Branch, and offices within the Department of Justice. OLC often deals with complex legal issues on which two or more agencies are in disagreement, and provides legal advice to the Executive Branch on constitutional questions, including the review of pending

legislation for constitutionality. Executive Orders proposed to be issued by the President are reviewed by OLC as to form and legality, as are other matters that require the President's formal approval. OLC also reviews proposed orders by the Attorney General and all regulations requiring the Attorney General's approval. (U)

B. Personnel Changes within Office of Legal Counsel (U)

John Yoo advised Attorney General Ashcroft and White House officials on the Stellar Wind program from the program's inception in October 2001 through Yoo's resignation from the Department in May 2003. Upon Yoo's departure, Patrick Philbin told the OIG that he was selected by the White House to assume Yoo's role as advisor to the Attorney General concerning the program.[111] With this personnel change came a fresh review of the legal underpinnings of the Stellar Wind program. We describe in the following sections the circumstances leading to what one official described as "the great rethink" of the program. ~~(TS//SI//NF)~~

1. Yoo's Role in the Program (October 2001 through May 2003) (U)

On September 11, 2001, and through November 2001, Daniel Koffsky was the Acting Assistant Attorney General for OLC. Koffsky was not read into the Stellar Wind program. Jay Bybee served as Assistant Attorney General for OLC from November 2001 until March 2003, when he became a judge on the U.S. Court of Appeals for the Ninth Circuit.[112] Bybee also was never read into the Stellar Wind program. As discussed in Chapter Three, John Yoo, a Deputy Assistant Attorney General in OLC, had sole responsibility within that office and within the Department of Justice for developing the legal analysis relating to the Stellar Wind program until May 2003.[113] Bybee told us he was not aware at the time that Yoo was drafting legal opinions in connection with a compartmented program. ~~(TS//SI//NF)~~

Bybee told us that the OLC normally adheres to a tradition called the "two Deputy rule," so that OLC opinions are reviewed by two OLC Deputy Assistant Attorneys General before going to the OLC Assistant Attorney General for approval. Bybee said that the purpose of this rule is to ensure

---

[111] On June 1, 2003, Philbin became an Associate Deputy Attorney General. However, he told us that he still technically remained a Deputy Assistant Attorney General in OLC and was thus "dual-hatted." (U)

[112] Bybee was nominated by President Bush to serve on the Ninth Circuit in May 2002 but was not confirmed by the Senate until March 2003. (U)

[113] Yoo's major opinions about electronic surveillance and Stellar Wind are summarized in Chapter Three. ~~(TS//SI//NF)~~

the quality of the legal research and soundness of the legal analysis. In addition, Bybee stressed that the Assistant Attorney General must be aware of all opinions that issue from the OLC. Bybee said that the OLC Assistant Attorney General has an obligation to "see the whole picture" and is the only person in the office who knows the full range of issues that are being addressed by the OLC. Bybee also said the Assistant Attorney General is the only official in that office who can assure that OLC opinions remain consistent. Bybee stated that the Assistant Attorney General, as a Senate-confirmed official, has ultimate accountability for the work of the office. Bybee noted that, by contrast, the Deputy Assistant Attorney General position, though political, does not require Senate confirmation. (U)

Bybee told the OIG that it would not be unusual for a Deputy Assistant Attorney General such as Yoo to have direct contact with the White House for the purpose of rendering legal advice. Bybee stated that it is "not clear" whether or to what extent the Attorney General needs to be kept informed of such contacts. However, Bybee said that the Attorney General may appropriately decide to ask a single OLC attorney to work on a particular project, but that it is "not the White House's call" to make such assignments because the White House may not be aware of what advice the OLC is providing to other Executive Branch agencies. Bybee told us that during his tenure as Assistant Attorney General he did not know that Yoo was working alone on a sensitive compartmented program, and he had no knowledge of how Yoo came to be selected for this responsibility. (U)

Philbin said he believed that White House Counsel Gonzales and Vice President Cheney's Counsel David Addington had selected Yoo to draft the OLC's opinions on Stellar Wind and other national security programs, and that Yoo was the "obvious choice" to assume this role because of his expertise in war powers issues and the authority of the Commander-in-Chief.[114] ~~(S//NF)~~

Gonzales told the OIG he understood that Yoo had asked others within OLC to help out with specific legal issues during this period without telling them what they were being asked to assist with, and Yoo then aggregated that work into his memoranda concerning electronic surveillance and the Stellar Wind program. Gonzales also stated that Yoo did not consult with any experts outside the Department in drafting his memoranda.[115] ~~(TS//SI//NF)~~

---

[114] As discussed in Chapter Three, Yoo had been given responsibility for working on national security issues prior to the inception of the Stellar Wind program. (U)

[115] When Gonzales testified before the Senate Judiciary Committee on February 6, 2006, he stated that although he was not at the Department when the program commenced, "I suspect – in fact I'm fairly sure – that there were not discussions with

(Cont'd.)

As noted above, neither Yoo nor Ashcroft agreed to be interviewed for the OIG's investigation. Other witnesses gave the OIG various accounts of Yoo's interactions with Attorney General Ashcroft and with the White House concerning the program. Gonzales told us that Yoo regularly advised Ashcroft on the legal aspects of the program so that Ashcroft could continue to certify it as to form and legality. Gonzales also said that it was incumbent on Ashcroft as Attorney General to satisfy the Department's legal obligations regarding the program. Gonzales told us he thus understood Yoo's opinions as representing the opinions of the Department. However, Gonzales acknowledged that White House officials consulted with Yoo and sought his advice without going through the Attorney General or Bybee – Yoo's supervisor – although Gonzales also said they did not seek Department approval from Yoo concerning the Stellar Wind program. ~~(TS//SI//NF)~~

Other witnesses described their concerns regarding Yoo's direct contacts with the White House, and with Addington and Gonzales in particular. Philbin said he told Addington that Yoo's direct access to Addington on legal matters was "not a good way to run things," referring to the lack of oversight of an OLC Deputy Assistant Attorney General by a supervisor. Philbin stated that there was nothing wrong with assigning a project to a subordinate, but not without the head of the office knowing what the subordinate was doing. (U)

Jack Goldsmith told us that when he became the Assistant Attorney General for the Office of Legal Counsel in October 2003, he learned that Yoo's contacts with the White House had had the effect of cutting the Attorney General "out of the loop," a practice Goldsmith said he resolved not to continue with any OLC attorney. (U)

Goldsmith also told us the White House had wanted Yoo to replace Bybee as the Assistant Attorney General for the Office of Legal Counsel following Bybee's confirmation as a judge on the Ninth Circuit, but that Ashcroft blocked the move. Yoo resigned from the Department in May 2003.[116] (U)

---

outside expertise at the Department, although I don't know for sure." An NSA Associate General Counsel for Operations told the OIG that Yoo visited the NSA for a briefing about the program at some point after he had drafted his November 2, 2001, legal memorandum. ~~(TS//SI//NF)~~

[116] In addition to working on the legal analysis for the Stellar Wind program while at the Justice Department, Yoo also worked on at least one other project involving a Top Secret compartmented detainee interrogation program. In contrast to the Stellar Wind program, the OIG determined that at least three OLC attorneys, including Bybee and Philbin, worked on the program's legal analysis with Yoo or participated by supervising his work. In addition, attorneys from the Department's Criminal Division and from other

(Cont'd.)

2. Philbin Replaces Yoo (U)

Patrick Philbin joined the Department as a Deputy Assistant Attorney General in the Office of Legal Counsel on September 4, 2001.[117] He was read into the Stellar Wind program in late May 2003, just before Yoo left the Department. Philbin said that he, accompanied by Yoo, was read into the program by Addington in Addington's office in the Old Executive Office Building. Philbin told us that Addington provided an overview of the program, describing the two basic categories of collection as "content" and "meta data." Philbin said that later, based on his legal analysis of the Stellar Wind program, he developed the "three baskets" terminology to describe more specifically the three types of collections. ~~(TS//STLW//SI//OC/NF)~~

Philbin said he was told by Addington he was being read into the program because Yoo was leaving the Department and another attorney was needed to review the threat assessments that supported the Presidential Authorizations and to then advise the Attorney General on recertifying the program as to form and legality.[118] Philbin said he also was told that he and the Attorney General were the only Justice Department officials who were supposed to be involved in this "review and recertification" process. Philbin told us he was aware that OIPR Counsel James Baker had also been read into the program; however, Philbin stated that Addington told him he should not discuss the program with Baker and should only advise the Attorney General on the program. Philbin said he believed Addington did not want Philbin speaking with Baker about the program because Addington had always taken the position that the program should be kept as compartmented as possible.[119] ~~(TS//SI//NF)~~

---

agencies were regularly consulted by Yoo in his drafting of the legal memoranda on the legality of this program. Yoo told the Department's Office of Professional Responsibility that Attorney General Ashcroft determined who was allowed to work on the memoranda for the detainee interrogation program. Transcript of Interview of John Yoo by Office of Professional Responsibility, June 7, 2005, at 12. ~~(TS//STLW//SI//OC/NF)~~

[117] Prior to joining the Department Philbin had been at a private law firm and had specialized in telecommunications law. (U)

[118] When asked whether he had any knowledge of the program prior to being read in, Philbin said he did not, but he recalled that in the fall of 2001 he had a discussion with Yoo about some general electronic surveillance issues. Yoo told Philbin that Yoo was told to work alone on this particular matter. Yoo did not state who had given him this instruction. ~~(TS//SI//NF)~~

[119] Baker told us he was not similarly advised to avoid discussions with Philbin about the program, nor was he aware that Addington had instructed Philbin not to discuss the program with him. In fact, according to Baker, Philbin initiated several conversations with Baker about the operational details of the program as Baker understood them at the time. (U)

The day after being read into the program, Philbin moved from the Office of Legal Counsel to the Office of the Deputy Attorney General to become an Associate Deputy Attorney General, although technically he still retained his OLC Deputy Assistant Attorney General position and was thus "dual-hatted." Philbin took over the "national security portfolio" from David Kris, who had recently left the Department. Philbin stated he was "somewhat concerned" that he would be advising the Attorney General on the Stellar Wind program even though Deputy Attorney General Larry Thompson, Philbin's supervisor, was not read into the program. However, Philbin said he anticipated at the outset that his work on the program would not require a lot of his time. ~~(S//NF)~~

3. Initial Concerns with Yoo's Analysis (U)

Philbin said that after he was read into the Stellar Wind program he believed he needed to do "due diligence" to learn about the program. He said he reviewed Yoo's legal opinions about the program and realized that Yoo had omitted from his analysis any reference to the FISA provision allowing the interception of electronic communications without a warrant for a period of 15 days following a congressional declaration of war. See 50 U.S.C. § 1811. Philbin also stated that Yoo's OLC opinions were premised on the assumption that FISA did not expressly apply to wartime operations, an assumption that from Philbin's perspective rendered the opinions "problematic." Philbin said that this gap in Yoo's analysis was his first indication that the legal reasoning underpinning the Presidential Authorizations would have to be revisited. ~~(TS//STLW//SI//OC/NF)~~

Philbin said the second indication of problems with Yoo's analysis came when he read a summary document Yoo had prepared concerning the program. [redacted]

[redacted]

Second, and more significantly, Philbin stated that [redacted]

[redacted] [120] ~~(TS//STLW//SI//OC/NF)~~ [redacted]

[redacted]

[120] See Presidential Authorization of April 22, 2003 at para. 4(b)(i) & (ii). The April 22, 2003, Authorization was the only Authorization personally approved as to form and legality by Yoo. He approved the Authorization on April 18, 2003, five days before the date of his talking points memorandum. ~~(TS//STLW//SI//OC/NF)~~

[12] [redacted]

[redacted]

Philbin said the errors in the Yoo's talking points document represented "a significant step toward the realization that the whole legal analysis was screwed up." Philbin told us he felt he could not rely on the existing analysis and that he needed to "build from the ground up." ~~(TS//SI//NF)~~

4. Problems with [redacted] ~~(TS//STLW//SI//OC/NF)~~

In addition to the flaws Philbin identified in Yoo's legal analysis, Philbin told us he grew increasingly concerned that [redacted] ~~(TS//STLW//SI//OC/NF)~~

[122] Philbin told us he visited the NSA three times during the summer of 2003 in an effort to learn how the program operated. Several officials we interviewed told us that Philbin understood the program well, in part due to his background in telecommunications law. (U//~~FOUO~~)

[redacted]

[redacted]

Philbin said that he and later Goldsmith recognized that the existence of the Stellar Wind program would be disclosed at some point in the future.

[redacted]

[redacted][123] ~~(TS//STLW//SI//OC/NF)~~

5. Other Collection Concerns ~~(S//NF)~~

Philbin told us that during the summer of 2003 he identified other concerns about the Stellar Wind program. First, Philbin said he began to believe that the existing OLC memoranda failed to describe the [redacted] Philbin said he also had concerns over [redacted] ~~(TS//STLW//SI//OC/NF)~~

6. Decision to Draft New OLC Memorandum (U)

In August 2003, Philbin brought his concerns about the OLC legal opinions to Attorney General Ashcroft. Philbin told Ashcroft that there were problems with the legal analysis supporting the program but probably not with the conclusions reached. Philbin told us that he believed that since the conclusions would not change there would be no need to "pull the plug" on the analytically problematic aspects of the program. Philbin said he

[redacted]

therefore advised that Ashcroft could continue to certify the program "as to form and legality." ~~(TS//SI//NF)~~

However, Philbin also recommended that a new OLC memorandum be drafted. According to Philbin, Ashcroft concurred, told him to continue working on his analysis, and asked to be kept updated on Philbin's progress. After meeting with Ashcroft to discuss the issue, Philbin said he began to write a new memorandum on the legality of the entire Stellar Wind program.[125] ~~(TS//SI//NF)~~

C. Reassessment of Legal Rationale for the Program ~~(TS//SI//NF)~~

1. Goldsmith Becomes OLC Assistant Attorney General (U)

Jack Goldsmith told the OIG that he was recommended for the Assistant Attorney General position by Yoo after Yoo was not selected for the position. Goldsmith stated that during his interview for the position, Attorney General Ashcroft and Ashcroft's Chief of Staff David Ayres emphasized that the OLC Assistant Attorney General must keep the Attorney General informed of matters the Office of Legal Counsel was working on and stressed the importance of keeping the Attorney General "in the loop." Goldsmith told the OIG that he believed Ashcroft and Ayres raised these issues as a result of their experience with Yoo. (U)

Goldsmith was selected for the position, confirmed by the Senate, and on October 6, 2003, was sworn in as the OLC Assistant Attorney General. (U)

According to Goldsmith, he was told by Department colleagues that the procedures OLC historically followed in drafting its opinions were changing and that the Attorney General was being circumvented in the new

---

[125] Philbin said that he was not certain at the time that Ashcroft fully understood the [redacted] because the subject matter was "difficult." Philbin also stated that for "client management" purposes, he needed to first make sure that he too fully understood the issues before raising his concerns to others. He said he did not just want to be "a naysayer" identifying problems, but also wanted to propose solutions. He said that the program would be examined by Congress one day and that the legal analysis had to be "carefully done to protect the President." Philbin said he therefore believed that the OLC legal memoranda had to be rewritten to achieve that objective. Philbin told us he also was concerned that the program not appear like a "rogue operation," but rather as a responsible approach to collecting intelligence with adequate controls and oversight. In this regard, Philbin emphasized that it would be important to demonstrate that the program had appropriate restrictions based on the law, and that the restrictions guarded against abuses. ~~(TS//SI//NF)~~

process. Goldsmith said that OLC Principal Deputy Assistant Attorney General Ed Whelan also told him that OLC's procedures, built on custom and practice but still "hugely important," had "broken down" prior to Goldsmith's arrival as the Assistant Attorney General. (U)

Goldsmith told us that he also became aware that Ashcroft sensed there was a White House-Office of Legal Counsel relationship over which Ashcroft did not have full control. Goldsmith said that when he became the OLC Assistant Attorney General he immediately moved to "bring things back to normalcy" by, for example, making sure all OLC memoranda were provided to client agencies for review and input and that all memoranda were reviewed by two OLC deputies, as was the traditional OLC practice.[126] (U)

With regard to the Stellar Wind program, Philbin told us he had always intended to request that Goldsmith be read into the program after Goldsmith was confirmed by the Senate. Philbin said that he went to the White House and asked Addington (and possibly Gonzales) to have Goldsmith read into the program. Philbin stated that Addington told him that he would have been "fine" with not allowing Goldsmith to be read in, and that Philbin would have to justify the request before Addington would convey the request to the President. Philbin told us he explained to Addington that he would need to have the head of OLC sign off on the new memorandum he was writing or the memorandum would lack credibility. (U//~~FOUO~~)

On November 17, 2003, Goldsmith was read into the Stellar Wind program by Addington in Addington's office.[127] Philbin was also present. On the way to the read-in, Philbin told Goldsmith to "prepare for your mind to be blown." Goldsmith told us that the read-in took approximately 5 minutes, and when it was over he remarked to Philbin, "That doesn't seem

---

[126] Goldsmith's view of how the OLC should operate was later echoed by a subsequent head of the office, Steven Bradbury. In a May 16, 2005, internal OLC guidance memorandum entitled "Best Practices for OLC Opinions," Bradbury emphasized that OLC legal memoranda should reflect the positions and expertise of interested agencies, and he also stressed the importance of a rigorous peer review process within the office before finalizing OLC memoranda. (U)

[127] After Ashcroft, Yoo, Baker, and Philbin, Goldsmith was only the fifth non-FBI Justice Department official to be read into the Stellar Wind program since the program's inception over 2 years earlier. Philbin stated that prior to Goldsmith's arrival at the Department and subsequent read-in to the program, he had no one to help him draft a new legal memorandum and no one other than Ashcroft with whom to discuss the legal issues. He told the OIG that it was extremely beneficial to have another attorney working with him on the project. Philbin also told us he did not press the White House to read in additional attorneys during the summer 2003 period before Goldsmith arrived at the Department. ~~(TS//SI//NF)~~

so bad." Goldsmith said that 3 weeks later, after studying the matter, he would come to a "different conclusion." (U//~~FOUO~~)

2. NSA Denied Access to OLC Memoranda (U//~~FOUO~~)

One of the first Stellar Wind meetings Goldsmith and Philbin attended after Goldsmith's read-in was held in the DOJ Command Center with Addington, NSA Deputy General Counsel Vito Potenza, and NSA Inspector General Joel Brenner. Goldsmith stated that the NSA Inspector General requested a copy of the OLC legal memoranda regarding the program as part of an audit the NSA Office of the Inspector General wanted to conduct of the program. According to Goldsmith, Addington "bit [the Inspector General's] head off," and made it clear that the memoranda would not be provided to the NSA OIG. ~~(TS//SI//NF)~~

Goldsmith said he learned either at that meeting or shortly thereafter that NSA's Office of General Counsel also had been denied access to the OLC memoranda. Bob Deitz, the NSA General Counsel during this period, told the NSA OIG that he was never permitted to see Yoo's legal memoranda. Dietz stated that he called Addington several weeks after the first Presidential Authorization was signed and asked if he could see a copy of Yoo's memorandum (likely the November 2, 2001, memorandum), and that Addington responded "no." Dietz said that Addington would only read "a paragraph or two" from the memorandum to him over a classified telephone line. Deitz stated that he never advised Yoo on his legal analysis, although he did advise NSA Director Hayden that he thought the program was legal and within the President's authority. ~~(TS//SI//NF)~~

The OIG also interviewed [redacted] the NSA's Associate General Counsel for Operations during Yoo's and Goldsmith's tenure in OLC. [redacted] told us that he was not troubled by the fact that other senior NSA officials had been denied access to Yoo's legal memoranda, and that he felt no need to review them. [redacted] stated that his primary concern with respect to the legality of the program was whether "Justice was comfortable with it." [redacted] also stated that he assumed that the Justice Department would find the program legal by resolving the tension between FISA and the President's inherent Commander-in-Chief authority based upon the doctrine of constitutional avoidance. ~~(TS//STLW//SI//OC/NF)~~

Goldsmith told us he found it "shocking" that the NSA was not provided access to Yoo's legal memoranda. He stated that the decision to withhold the memoranda was one of the "most astonishing things" he learned about how the program was handled, and that he could not "draw a good inference" from that fact. Goldsmith emphasized that under the Stellar Wind program the NSA had been asked to do something contrary to its ordinary practices, and yet was not allowed to review the legal

justifications for being permitted to do it. Goldsmith told us he believed that the NSA might have identified problems or mistakes in Yoo's analysis early in the program had it been given access to his memoranda. ~~(TS//SI//NF)~~

Goldsmith told us that upon becoming the Assistant Attorney General he intended to reverse the practice of keeping OLC memoranda closely held, and that he also decided he would seek client agency expertise in drafting these documents. (U)

3. Goldsmith Joins Effort to Reassess Legal Basis for the Program ~~(TS//SI//NF)~~

In the two or three weeks following his read-in to the Stellar Wind program, Goldsmith reviewed several documents to educate himself about the program. These included the memorandum that Philbin had already begun to draft (which included a description of how the program worked operationally), Yoo's memoranda, and older OLC memoranda concerning surveillance activities. After Goldsmith familiarized himself with the program, Goldsmith provided Philbin with additional research and helped supplement Philbin's draft memorandum. ~~(TS//STLW//SI//OC/NF)~~

Goldsmith stated that Philbin had done an "amazingly heroic job" in reviewing the program. Goldsmith believed "ninety-nine out of a hundred" attorneys in Philbin's position, having been asked simply to opine as to form and legality, would have just relied on the previous Office of Legal Counsel memoranda. Goldsmith said that Philbin, however, was not convinced by those memoranda and therefore did not rely on them. In addition, Goldsmith noted that Philbin sought to understand the program as it was actually implemented at the NSA before advising the Attorney General on its legality. ~~(TS//SI//NF)~~

[redacted]

128 [redacted]

(Cont'd.)

[redacted] ~~(TS//STLW//SI//OC/NF)~~

4. AUMF Becomes the Primary Legal Rationale Supporting [redacted] of the Stellar Wind Program ~~(TS//STLW//SI//OC/NF)~~

[redacted]

Goldsmith concluded the NSA's interception of [redacted] did not comply with FISA's requirement to obtain judicial authorization, and did not fall within any of the exceptions to this requirement. Goldsmith later wrote in his legal memorandum reassessing the legality of the program that a proper analysis

[redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[130] See Goldsmith's May 6, 2004, memorandum entitled "Review of the Legality of the Stellar Wind Program" (Goldsmith Memorandum, May 6, 2004). This memorandum is discussed in Section II C below. ~~(TS//STLW//SI//OC/NF)~~

of Stellar Wind "must not consider FISA in isolation" but rather must consider whether Congress, by authorizing the use of military force against al Qaeda, also "effectively exempts" such surveillance from FISA. Goldsmith concluded that this reading of the AUMF was correct because the AUMF authorized the President to use "all necessary and appropriate force" against the enemy that attacked the United States on September 11, 2001, and to "prevent any future acts of international terrorism against the United States" by such enemy – authority that has long been recognized to include the use of signals intelligence as a military tool. ~~(TS//STLW//SI//OC/NF)~~

Alternatively, Goldsmith reasoned that even if the AUMF did not exempt surveillance under the program from the restrictions imposed by FISA, the question was sufficiently ambiguous to warrant the application of the doctrine of constitutional avoidance, and therefore should be construed not to prohibit the activity.[131] ~~(TS//STLW//SI//OC/NF)~~

[redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[131] In his May 6, 2004, memorandum, Goldsmith concluded that if the [redacted] arguments under the AUMF did not create sufficient ambiguity as to trigger the doctrine of constitutional avoidance, FISA as applied would represent an unconstitutional infringement on the President's exclusive authority as Commander-in-Chief in wartime to protect the nation from attack. ~~(TS//STLW//SI//OC/NF)~~

[redacted]

5. Office of Legal Counsel Raises its Reassessment of the Stellar Wind Program (December 2003 through January 2004)[133] ~~(TS//SI//NF)~~

During late 2003, Goldsmith and Philbin continued their analysis of the legal bases for the Stellar Wind program. During this time Philbin and Goldsmith were the only two Department officials in a position to brief the Attorney General and White House officials on the status of their legal reassessment and its potential ramifications for the operation of the program.[134] ~~(TS//SI//NF)~~

With the existing Presidential Authorization set to expire on December 11, 2003, Goldsmith and Philbin met with Ashcroft on December 8, 2003, to advise him on recertifying the program as to form and legality. Goldsmith wrote in notes that he maintained during this time period that at the meeting he and Philbin "note[d] problems gently" to Ashcroft. Goldsmith told us Ashcroft was "extraordinarily supportive" of his and Philbin's efforts to reassess the legality of the program and made clear his view that the program had to be on solid legal footing. ~~(TS//STLW//SI//OC/NF)~~

Goldsmith advised Ashcroft that, despite concerns about the program, Ashcroft should certify the December 9, 2003, Authorization. Goldsmith

[redacted]

[132] [redacted]

[133] The narrative in this and the following sections is based on our interviews of Philbin, Goldsmith, Comey, Mueller, Gonzales, and others. We also relied on Philbin's and Goldsmith's contemporaneous notes, Goldsmith's chronology of events that he wrote during this period, Mueller's Program Log documenting events in March 2004, and Attorney General Ashcroft's FBI security detail log of events that occurred while Ashcroft was hospitalized from March 4 through March 14, 2004, among other documents. (U)

[134] James Comey became the Deputy Attorney General on December 9, 2003, but was not read into the program until over 2 months later. (U)

later advised Ashcroft to certify the January 14, 2004, Authorization as well. Goldsmith told us he made these recommendations to Ashcroft with the caveat that although he believed Yoo's memoranda to be flawed, Goldsmith had not yet concluded that the program itself was illegal. ~~(TS//SI//NF)~~

Based on Goldsmith's advice, Ashcroft certified the December 9, 2003, and January 14, 2004, Authorizations. ~~(TS//SI//NF)~~

In December 2003 Philbin and Goldsmith informed Ashcroft that they believed Comey, who was sworn in as the new Deputy Attorney General in December 2003, also needed to be read into the program. Philbin said he justified this request by noting that he would be traveling abroad for 2 weeks later that month on an unrelated Justice Department matter.[135] (U)

In December 2003, Goldsmith and Philbin met with Addington and Gonzales at the White House to express their growing concerns about the legal underpinnings for program. Goldsmith said he told them that OLC was not sure the program could survive in its current form. According to Goldsmith's notes, these discussions did not contemplate an interruption of the program, although the White House represented that it would "agree to pull the plug" if the problems with the program were found to be sufficiently serious. Goldsmith told us that the White House – typically through Addington – told him "several times" that it would halt the program if the Department found that it could not be legally supported. ~~(TS//SI//NF)~~

Philbin told us he recalled that Addington in particular was "annoyed" with the OLC's preliminary conclusion that [redacted] Philbin said that Addington nevertheless told him and Goldsmith to continue analyzing the program and that if serious problems were found, the program would be shut down. ~~(TS//STLW//SI//OC/NF)~~

On December 18, 2003, while Philbin was abroad, Goldsmith met again with Addington and Gonzales. Goldsmith wrote in his chronology that this time he conveyed with "more force" his "serious doubts and the need to get more help to resolve the issue [as soon as possible]." Goldsmith also told Addington and Gonzales that he needed more resources to continue examining the legality of the program. They responded to this request by telling Goldsmith that Philbin should devote all of his time to the project.

---

[135] As discussed in Chapter Three, Comey's predecessor as Deputy Attorney General, Larry Thompson, was never read into the Stellar Wind program despite Ashcroft's request to the White House on behalf of both Thompson and Ashcroft's chief of staff. (U//~~FOUO~~)

Goldsmith told us that he asked to have Comey read into the program. According to Goldsmith's notes, Addington and Gonzales "bristle[d]" at that suggestion. Goldsmith told us he made the request for Comey to be read in because he believed he would need the Deputy Attorney General's assistance to help "make the case" to the White House that the program was legally flawed. Goldsmith also stated that he wanted Comey read in because, as the Deputy Attorney General, Comey was Philbin's direct supervisor. ~~(TS//SI//NF)~~

We asked Gonzales when he first became aware that the Department had concerns about the legality of the Stellar Wind program. Gonzales stated that he remembered that sometime after Philbin and Goldsmith joined the Department, they decided to conduct a programmatic review of the legal basis for Stellar Wind. Gonzales said that he welcomed this review, and that it was always important to reassess the value of or need for the program, as well as its legality. Gonzales told us he thought that Goldsmith and Philbin's review arose out of concerns about Yoo's November 2, 2001, opinion and that their review was limited to that document. Gonzales said that Goldsmith periodically told him that Philbin was reviewing the program and that some questions had been raised or that some changes to the program might be needed as a result of their reassessment. Gonzales said that he told Goldsmith to let him know how the review was progressing. Gonzales also told us he did not recall getting into any specific discussions with Goldsmith about OLC's concerns until early March 2004. ~~(TS//SI//NF)~~

In contrast, Goldsmith told us he had been "crystal clear" with Gonzales and Addington that the Office of Legal Counsel had concerns about the legality of aspects of the program as early as December 2003, although Goldsmith also acknowledged that his discussions with Gonzales and Addington became more detailed in March 2004. Goldsmith told us that he gave the two White House officials the same caveats he gave Ashcroft when advising him on the legality of the program – that there were flaws in Yoo's analysis, but that OLC had not yet concluded that the program itself was illegal. ~~(TS//SI//NF)~~

Goldsmith's efforts to gain the White House's permission to have others (including Comey) read into the program continued through January 2004. According to Goldsmith's notes, both Addington and Gonzales pressed Goldsmith on his reason for the request and continued to express doubt that additional resources were needed. However, in late January the White House agreed to allow Comey to be read in, provided that Philbin devoted all of his time to his analysis of the program and, according to Goldsmith, that the Department's legal analysis be completed by March 2004 when the Presidential Authorization was due to be renewed. (U)

6. Deputy Attorney General Comey is Read into the Program (U)

Comey became the Deputy Attorney General on December 9, 2003, and was read into the Stellar Wind program on February 17, 2004. Comey told us that he had no awareness of the program prior to being read in. He said he learned after his read-in that Addington had resisted Goldsmith and Philbin's efforts to have him read in earlier. Comey said Addington was the "gatekeeper" for Stellar Wind and wanted to keep the program a "close hold." (U)

Comey told us that NSA Director Hayden personally wanted to conduct Comey's read-in to the program. Hayden read in Comey at the Justice Command Center in a briefing that took approximately 20 to 30 minutes. Comey said that, at the read in, Hayden explained the "three baskets" to him. ~~(TS//STLW//SI//OC/NF)~~

Comey told us that after Hayden left the Command Center, Comey and Philbin continued discussing the program. Philbin told Comey that there were problems with the legality of the program and that there were "operational issues" as well. Comey told us that his initial reaction to the program was "unprintable." He said he thought that the NSA could not collect the content of certain communications covered by the program outside of FISA authority. Hayden told the OIG that Comey raised no objections to him about the program upon being read in. (U)

Within the first month after being read in, Comey discussed the program with Ashcroft, Goldsmith, Philbin, and other Department officials who had been read in by this time, including James Baker, Counsel for Intelligence Policy; Chuck Rosenberg, Comey's Chief of Staff, and Daniel Levin, Counsel to the Attorney General.[136] Comey said he did not recall having any discussions about the program with FBI Director Mueller during this period. (U)

Comey also recalled meeting with Scott Muller, the CIA General Counsel, shortly after being read into the program. Comey said that he told Muller about the legal concerns Philbin and Goldsmith had raised regarding Yoo's analysis and that Muller agreed that the concerns were well founded. (U)

Comey also told us that Goldsmith had identified for Comey as a particular concern the notion that Yoo's legal analysis entailed ignoring an

---

[136] Levin had just returned to the Department after working in private practice and serving as a Bush Administration liaison to the September 11 Commission. Rosenberg was read into Stellar Wind in 2003 while serving as Counsel to FBI Director Mueller. (U)

act of Congress, and doing so in secret. Comey stated that Goldsmith described such action as "breathtaking." Comey agreed, describing the action as "unprecedented." (U)

D. Office of Legal Counsel Presents its Conclusions to the White House (U)

On March 1, 2004, Philbin completed a first draft of a revised OLC opinion on the Stellar Wind program. According to Goldsmith's notes, at this time Goldsmith and Philbin had not yet concluded "definitively" that there was "anything certainly wrong" with the program, with the possible exception of the scope of [redacted] ~~(TS//STLW//SI//OC/NF)~~

In explaining the rationale for the revised opinion, Comey described to the OIG his view of two approaches or standards that could be used to undertake legal analysis of government action. If the government is contemplating taking a particular action, OLC's legal analysis will be based on a "best view of the law" standard. However, if the government already is taking the action, the analysis should instead focus on whether reasonable legal arguments can be made to support the continuation of the conduct.[137] Comey said that because Stellar Wind was an ongoing program, Goldsmith and Philbin's analysis proceeded under the second approach. Under this approach, at this point they concluded that there were reasonable legal arguments to be made to continue the collection of [redacted] but they still had not identified a legal argument to support [redacted] ~~(TS//STLW//SI//OC/NF)~~

Comey said that during early March 2004 the sense was that "we can get there" as to [redacted] albeit by using an aggressive legal analysis. However, he said that collection of [redacted] would require [redacted] ~~(TS//STLW//SI//OC/NF)~~

[137] Goldsmith emphasized to us that this second situation almost never presents itself, and that OLC rarely is asked to furnish legal advice on an ongoing program because the pressure "to say 'yes' to the President" invariably would result in applying a lower standard of review. Goldsmith stated that OLC's involvement in Stellar Wind was "unprecedented" because OLC is always asked to review the facts and formulate its advice "up front." ~~(S//NF)~~

On March 1, 2004, Comey met with FBI Director Mueller to inform him that the OLC had found problems with the legal authority for the Stellar Wind program, particularly with the [redacted] According to a log Mueller kept documenting events in March 2004 concerning the program, Comey said he was trying to work out these problems with the OLC and "other interested parties."[138] Mueller told us that March 1, 2004, was when he first became aware of the Department's concerns about the legal support for the program. Mueller described the FBI as "recipients of information from the program," and that the dialogue as to the program's legality was between the Department and the White House. ~~(TS//STLW//SI//OC/NF)~~

1. March 4, 2004: Comey Meets with Ashcroft to Discuss Problems with the Program (U)

Comey told us he met with Attorney General Ashcroft for lunch on March 4, 2004, to discuss the Stellar Wind program. Comey reminded Ashcroft of the details of the program and said he used salt and pepper shakers and a knife to represent the three baskets during the discussion. According to Comey, Ashcroft agreed with Comey and OLC's assessment of the potential legal problems, and he instructed Comey to "just fix it" and "tell them to make the changes that need to be done." ~~(TS//STLW//SI//OC/NF)~~

Comey said he assumed Ashcroft meant that Comey should reach out to the NSA and the White House for the necessary changes. The Presidential Authorization in effect at the time was due to expire on March 11, 2004. Comey said Ashcroft did not discuss with him whether he would recertify the program as it was currently being authorized by the President. ~~(TS//SI//NF)~~

Comey also described Ashcroft as being frustrated, and said he was "beating himself up" because he was "in a box" with Yoo, yet was learning from Philbin, Goldsmith, and now Comey that parts of the program were not in their view legally supportable.[139] ~~(TS//SI//NF)~~

After the lunch meeting on March 4, Comey traveled to Phoenix, Arizona, to make a speech. Three hours after their lunch meeting, Ashcroft was struck with severe gallstone pancreatitis and was admitted to the

---

[138] Mueller told us he maintained the program log because "[t]hese were extraordinary circumstances about which I would one day be questioned." Mueller said the program log was drafted "relatively contemporaneously" with the events described in it. (U)

[139] By the time Ashcroft received OLC's preliminary findings concerning the legality of the program in December 2003, he had already certified the program as to form and legality approximately 20 times. ~~(TS//SI//NF)~~

George Washington University Hospital. After being informed that Ashcroft was hospitalized, Comey returned to Washington the next morning on an FBI jet. (U)

2. March 5, 2004: Comey Determines Ashcroft is "Absent or Disabled" (U)

On March 5, 2004, Goldsmith advised Comey by memorandum that under the circumstances of Ashcroft's medical condition and hospitalization, a "clear basis" existed for Comey to determine that "this is a case of 'absence or disability' of the Attorney General" within the meaning of 28 U.S.C. § 508(a). This statute provides:

> In case of a vacancy in the office of Attorney General, or of his absence or disability, the Deputy Attorney General may exercise all the duties of that office, and for purposes of section 3345 of title 5 the Deputy Attorney General is the first assistant to the Attorney General. (U)

Goldsmith's memorandum further advised Comey that he could serve as Acting Attorney General until Ashcroft's absence or disability no longer existed, and that Comey could exercise "all the power and authority of the Attorney General, unless such power or authority is required by law to be exercised by the Attorney General personally." See 28 C.F.R. § 0.15(a). Goldsmith noted in the memorandum that there are "very few duties" that can be exercised only by the Attorney General. Goldsmith wrote that, except for these duties, Comey could opt to exercise the duties of the Attorney General as Deputy Attorney General rather than as Acting Attorney General, noting, "Your office has informed us that this is your intention."[140] (U)

Goldsmith's memorandum to Comey referenced an attached draft memorandum for Comey's review, which would memorialize Comey's decision to invoke 28 U.S.C. § 508(a) in writing, although Goldsmith advised that it was not necessary to do so. The "cc" line of Goldsmith's memorandum to Comey indicated that a copy of the memorandum was also

---

[140] According to an e-mail sent on March 5, 2004, at 9:15 a.m. from OLC Special Counsel Daniel Koffsky to OLC Principal Deputy Assistant Attorney General Edward Whelan and other Department officials, among the duties that can only be exercised by the Attorney General or his designee is the authority to approve FISA applications to engage in electronic surveillance of a specific type of agent of a foreign power based on requests of certain high level officials. 50 U.S.C. § 1804(e)(2)(A). This section represents an exception to FISA's general conferral of authority on the Attorney General, a term that is defined to include the Acting Attorney General and the Deputy Attorney General. See 50 U.S.C. § 1801(g). (U)

sent to White House Counsel Gonzales.[141] As discussed below, a significant dispute between White House and Department officials later arose over whether the White House in fact received notice of Comey's decision to assume the powers of the Attorney General, whether as Deputy Attorney General or otherwise. (U)

3. March 5, 2004: Goldsmith and Philbin Seek Clarification from White House on Presidential Authorizations (U)

On the afternoon of Friday, March 5, 2004 – 6 days before the Presidential Authorization then in effect was set to expire – Goldsmith and Philbin met with Addington and Gonzales at the White House to seek clarification on two key issues related to the Authorizations. (U//~~FOUO~~)

First, Goldsmith expressed his belief that the [redacted] Philbin said they explained to Addington and Gonzales the importance of briefing the President on this new legal approach to justifying the program. ~~(TS//STLW//SI//OC/NF)~~

Second, [redacted] ~~(TS//STLW//SI//OC/NF)~~

---

[141] A March 12, 2004, e-mail from Ashcroft's Chief of Staff David Ayres to Deputy White House Counsel David Leitch detailing the Department's efforts to inform the White House Counsel's Office of Ashcroft's hospitalization and Comey's assumption of Ashcroft's duties shows that Ayres confirmed the White House's receipt of a facsimile from OLC advising the White House of Comey's decision to exercise "all the power and authority of the Attorney General . . . in [his] capacity as Deputy Attorney General." Ayres also wrote in the e-mail that a copy of OLC's "legal memorandum" was sent to White House Counsel Gonzales. Ayres also wrote in the e-mail that he personally called Harriet Miers, a White House Deputy Chief of Staff, and informed her that Comey "had assumed the Attorney General's responsibilities[.]" Ayres wrote in the e-mail that he also informed others at the White House of Comey's status, including another White House Deputy Chief of Staff [Joe Hagin] and the White House Cabinet Secretary [Brian Montgomery]. (U)

[redacted]

However, according to Gonzales, Goldsmith's conclusion [redacted] created a serious issue. Gonzales stated that Goldsmith's argument on this point was that Congress had spoken on the matter by enacting FISA, but Yoo previously had opined that FISA was unconstitutional to the extent it infringed on the President's Commander-in-Chief authority to conduct electronic surveillance without a judicial warrant.[142] ~~(TS//STLW//SI//OC/NF)~~

Gonzales also told us that the March 5, 2004, meeting with Goldsmith and Philbin represented the first substantively detailed discussion he had with the OLC officials regarding their concerns with the existing legal analysis and their reservations about continuing the program as it had been operating. As noted above, Goldsmith said that he had informed Gonzales and Addington about his general concerns with Yoo's legal analysis of the program as early as December 2003. ~~(TS//SI//NF)~~

Later that day on March 5, Gonzales called Goldsmith to request a letter from the OLC stating that Yoo's prior OLC opinions "covered the program." Philbin told the OIG that Gonzales was not requesting a new

[redacted]

[142] [redacted]

opinion that the program itself was legal, but only that the prior opinions had concluded that it was. ~~(TS//SI//NF)~~

4. March 6 to 8, 2004: The Department Concludes That Yoo's Legal Memoranda Did Not Cover the Program (U)

As a result of Gonzales's request on March 5, Goldsmith re-examined Yoo's memoranda with a view toward determining whether they adequately described the actual collection activities of the NSA under the Authorizations. Goldsmith told us that after a brief review, he called Philbin to tell him he agreed with Philbin's assessment that Yoo's memoranda were problematic from a factual standpoint. Philbin said that through this re-examination he and Goldsmith confirmed Philbin's initial sense that Yoo's memoranda did not describe the [redacted] 143 ~~(TS//STLW//SI//OC/NF)~~

[redacted]

Goldsmith's account of the response to Gonzales's request was similar. Goldsmith also stated that his and Philbin's conclusion that Yoo's memoranda failed to adequately describe the [redacted] meant that OLC could not tell the White House that the program could continue under the authority of those legal memoranda. Goldsmith stated that he and Philbin realized at this point that the program had been conducted for 2 years without a proper OLC review. Specifically, both Goldsmith and Philbin stated that they had always viewed Yoo's legal analysis as poorly reasoned; however, they were now realizing that Yoo's factual description of the program was inaccurate and incomplete as well, and thus did not "cover" aspects of the program. Goldsmith said Gonzales's request for ratification of Yoo's memoranda "forced [the Office of Legal

143 [redacted]

Counsel's] hand" and was the point at which the "presumption in favor of legality flipped."[144] ~~(TS//STLW//SI//OC/NF)~~

On Saturday, March 6, 2004, Goldsmith and Philbin advised Comey that they believed the [redacted] Goldsmith also told Comey that the White House would have to be notified of this development. Comey agreed with this recommendation. ~~(TS//STLW//SI//OC/NF)~~

Later on March 6, Goldsmith and Philbin went to the White House to meet with Addington and Gonzales to convey their conclusions that the [redacted] According to Goldsmith's chronology of these events, Addington and Gonzales "reacted calmly and said they would get back with us." Goldsmith told us that the White House was now worried that it was "out there," meaning that it was implementing a program without legal support. ~~(TS//STLW//SI//OC/NF)~~

On Sunday afternoon, March 7, 2004, Goldsmith and Philbin met again with Addington and Gonzales at the White House.[145] According to Goldsmith, the White House officials informed Goldsmith and Philbin that they disagreed with Goldsmith and Philbin's interpretation of Yoo's memoranda and on the need to change the scope of the NSA's collection.[146] Gonzales told us he recalled the meetings of March 6 and 7, 2004, but did not recall the specifics of the discussions. He said he remembered that the overall tenor of the meetings with Goldsmith was one of trying to "find a way forward."[147] ~~(TS//SI//NF)~~

---

[144] As noted in Chapter Three, Gonzales told us that he believed Yoo's memoranda described as lawful activities that were broader than those carried out under Stellar Wind, and that therefore these opinions "covered" the Stellar Wind program. ~~(TS//SI//NF)~~

[145] Gonzales told us that White House Chief of Staff Card may also have been present for this meeting. Goldsmith's chronology indicates that only Addington and Gonzales were present. (U)

[146] In discussing these early March meetings with the OIG, Goldsmith told us that Addington had stated on more than one occasion that Goldsmith was the head of OLC and if he determined that the program needed to be shut down, it would be shut down. Goldsmith told us he believed that the White House officials' references to "shutting down the program" extended only to those aspects of the program for which no legal support could be found. Goldsmith also told us that he did not know whether Addington and Gonzales were keeping the President informed of OLC's concerns. ~~(TS//SI//NF)~~

[147] As noted above, Gonzales was represented by counsel during his interview with the OIG. Also present during the interview because of the issue of executive privilege was a Special Counsel to the President, Emmitt Flood. We asked Gonzales whether the President had been informed by this point in time of the OLC position regarding the lack of legal (Cont'd.)

On the evening of Sunday, March 7, 2004, Goldsmith and Philbin met with Comey in Comey's office to again review Yoo's opinions and make sure all three agreed with the conclusion that the opinions failed to support the Stellar Wind program as it was being implemented. Philbin said that until Gonzales's March 5 request for a letter from the OLC stating that Yoo's prior OLC opinions "covered the program," he and Goldsmith had intended to recommend that the program be recertified on March 11, 2004, while they continued to work on the new OLC opinion. [redacted]

~~(TS//STLW//SI//OC/NF)~~

According to Goldsmith's chronology, there was no interaction with the White House on the issue on the following day, Monday, March 8, 2004. Goldsmith wrote in his chronology of events for this day: "Monday, March 8: Silence." (U)

5. March 9, 2004: White House Seeks to Persuade Department and FBI to Support Continuation of the Program ~~(S//NF)~~

On Tuesday, March 9, 2004, Gonzales called Goldsmith to attend an early morning meeting (at 6:00 or 6:30 a.m.) at the White House to discuss the issues regarding Yoo's memoranda and the Stellar Wind program.[149] Goldsmith called Philbin and told him to meet Goldsmith at the White House. According to Goldsmith, Philbin was allowed into the White House, but Gonzales excluded Philbin from the meeting despite Goldsmith's requests that Philbin be allowed to participate. ~~(S//NF)~~

---

support for the program and [redacted]. Flood objected to the question on relevancy grounds and advised Gonzales not to answer, and Gonzales did not provide us an answer. However, when Gonzales commented on a draft of this report, he stated that he would not have brought Goldsmith and Philbin's "concerns" to the attention of the President because there would have been nothing for the President to act upon at that point. Gonzales stated that this was especially true given that Ashcroft continued to certify the program as to legality during this period. Gonzales stated he generally would only bring matters to the President's attention if the President could make a decision about them. ~~(TS//STLW//SI//OC/NF)~~

[148] [redacted]

[149] Gonzales told the OIG that he did not recall this meeting. Both Goldsmith and Philbin told the OIG about the meeting. The meeting is also briefly described in Goldsmith's contemporaneous notes and chronology. (U)

Goldsmith said Gonzales tried first to persuade him that he and Philbin were wrong to conclude that Yoo's memoranda did not provide sufficient legal justification to cover the parts of the program that OLC had identified as problematic, but that Gonzales did not persuade him on this point. Gonzales next argued for a "30-day bridge" to get past the upcoming March 11, 2004, Authorization. Gonzales reasoned that Ashcroft, who was still hospitalized, was not in any condition to sign the upcoming Authorization, and that a "30-day bridge" would move the situation to a point where Ashcroft would be well enough to approve the program. Goldsmith told Gonzales he could not agree to recommend an extension. ~~(TS//SI//NF)~~

Goldsmith said Gonzales noted that Ashcroft had certified the program as to form and legality for the previous two and a half years, yet now Comey was the Acting Attorney General. Goldsmith said the implication of Gonzales's statement was that not approving the March 11, 2004, Authorization would "undercut" Ashcroft. Goldsmith said he made clear to Gonzales that Ashcroft was "supportive" of his and Philbin's analysis. Goldsmith's notes from the meeting also indicate that Gonzales stated that he did not "want to face" Ashcroft in the hospital. Goldsmith told us he recommended to Gonzales that he not visit Ashcroft.[150] ~~(TS//SI//NF)~~

Goldsmith said his discussion with Gonzales lasted about 1 hour. Philbin was then brought into Gonzales's office and the issues were discussed again. According to Goldsmith's chronology, nothing was resolved during the meeting. (U)

At noon that day, another meeting was held in Andrew Card's office at the White House. According to Director Mueller's program log, Mueller, Chief of Staff Card, Vice President Cheney, CIA Deputy Director John McLaughlin, Hayden, Gonzales, and other unspecified officials were present. Comey, Goldsmith, and Philbin were not invited to this meeting. Mueller described this gathering as a "pre-meeting" in anticipation of another meeting that was to be held later that afternoon in which the Justice Department officials (Comey, Goldsmith, and Philbin) would be participating.[151] (U)

---

[150] At noon on March 9, 2004, Attorney General Ashcroft underwent surgery at the George Washington University Hospital. The surgery was completed by 2:30 p.m. (U)

[151] Mueller prepared for this meeting by meeting earlier that morning with Michael Fedarcyk, the Chief of the FBI's Communications Exploitation Section; General Counsel Valerie Caproni; and possibly others. Mueller's program log indicates that Fedarcyk "appears unaware of details of how [redacted] is collected." ~~(TS//SI//NF)~~

According to Mueller's notes, a presentation on the value of the Stellar Wind program was given by CIA and NSA representatives.[152] It was then explained to the group that Comey "has problems" with [redacted] Mueller's notes state that Vice President Cheney suggested that "the President may have to reauthorize without [the] blessing of DOJ," to which Mueller responded, "I could have a problem with that," and that the FBI would "have to review legality of continued participation in the program." ~~(TS//STLW//SI//OC/NF)~~

A third meeting was held at the White House that afternoon, at 4:00 p.m. The meeting included Comey, Goldsmith, and Philbin, in addition to Vice President Cheney, Card, Addington, Gonzales, Hayden, Mueller, CIA General Counsel Muller, McLaughlin, and approximately 10 NSA analysts. Gonzales told us the meeting was held to make sure that Comey understood what was at stake with the program and to demonstrate its value. ~~(S//NF)~~

At the beginning of the meeting the NSA analysts made a presentation to Comey, Goldsmith, and Philbin. Comey said the presentation consisted of charts showing the chaining [redacted] capabilities that could be generated from Stellar Wind-derived information, as well as a description of "success stories" resulting from the program. Comey told us that the cases the analysts highlighted were not in his view the Stellar Wind successes that the analysts claimed, and that he felt "the NSA had no good stories to tell about the program."[153] Comey also told us that the collection of content communications under Stellar Wind was somewhat duplicative of existing FISA coverage, and that only the meta data collection under baskets 2 and 3 represented truly new capabilities. However, Comey said he did not challenge the analysts on the assertion that Stellar Wind was a critical anti-terrorism tool because the value of the program was not his primary concern. Rather, Comey said he was willing to concede the program's value, and that his concern was with its legality. ~~(TS//STLW//SI//OC/NF)~~

Goldsmith told us that he did not believe it was his place to judge the value of the program from an intelligence-gathering standpoint. Goldsmith told us he found persuasive a remark by Hayden that even though there may not have been major successes under the program to date, the program still could produce successes in the future. However, both Goldsmith and

---

[152] Mueller's notes indicate that [redacted] were cited as examples during the presentation. We discuss [redacted] briefly in this chapter and [redacted] in Chapter Six. ~~(TS//STLW//SI//OC/NF)~~

[153] Comey specifically questioned whether the [redacted] case was a legitimate "success story" under the Stellar Wind program. The [redacted] case, as well as other cases cited as successes under Stellar Wind, is discussed in Chapter Six. ~~(TS//STLW//SI//OC/NF)~~

Philbin told us that they believed that identifiable successes under the program [redacted] ~~(TS//STLW//SI//OC/NF)~~

The NSA analysts were excused after their presentation and the meeting continued. Comey said Vice President Cheney stressed that the program was "critically important" and warned that Comey would risk "thousands" of lives if Comey did not agree to recertify it. Comey said he told those at the meeting that he, as the Deputy Attorney General exercising the powers of the Attorney General, could support reauthorizing [redacted].[154] However, he told the group "we can't get there" on [redacted] According to Comey, the White House said it could not agree to that modification. ~~(TS//STLW//SI//OC/NF)~~

Comey also told us he was certain the White House understood him to be the acting in Attorney General Ashcroft's stead during this meeting. (U)

[redacted]

Gonzales told us that he came away from the meeting with the understanding that Comey [redacted] ~~(TS//STLW//SI//OC/NF)~~

6. Conflict Ensues between Department and White House (U)

Each of the Department witnesses we interviewed concerning the Department's discussions with the White House during this time period

---

[154] [redacted]

emphasized the sense of pressure and anxiety that pervaded the discussions in March 2004. For instance, Comey said discussions during the meeting at the White House on March 9 became heated as he sought to convey to everyone how difficult it was for the Department to take the position it was taking, and how hard the Department officials were working to find a solution. Comey also stated that Vice President Cheney was "understandably frustrated" because the Department was changing its advice to the White House about the program. (U)

Goldsmith also recalled that at one point during these meetings with the White House, Addington told him that if he narrowed the Stellar Wind program Goldsmith "will have the blood of 100,000 American lives on his hands." ~~(S//NF)~~

Goldsmith observed to us that from the White House's point of view, due to the timing of the events, and in particular with Ashcroft in the hospital, it appeared to the White House that a "palace coup" was taking place at the Department of Justice. Goldsmith said that this perception was somewhat understandable under the circumstances. (U)

Philbin also stated that tensions were high during this period and that the Department and White House "started to divide into camps." Philbin added that Department and White House officials were "starting to attribute motives" to each other. Philbin said he thought Addington came to believe that Comey was opposed to recertifying the program for "political reasons," and that Comey wanted to be on the "politically right" side of the dispute. (U)

Comey said that his dealings with Gonzales, Card, Addington, and others at the White House were generally civil. Comey acknowledged that there was tension between the Department and the White House during the March 2004 period, but believed that it resulted primarily from differences in legal perspectives. (U)

II. White House Continues Program without Justice Department's Certification ~~(TS//SI//NF)~~

The Presidential Authorization under which the program was operating during early 2004 was set to expire on March 11, 2004. As described in the preceding section, Comey concurred with the views of Goldsmith and Philbin, and as the Deputy Attorney General exercising the powers of the Attorney General Comey refused to certify the program as to form and legality. He conveyed this decision to the White House during the meeting on the afternoon of March 9, 2004. In response, as described below, the President decided to reauthorize the program without the Justice

Department's support, precipitating a serious confrontation between White House and Department officials. ~~(TS//STLW//SI//OC/NF)~~

A. White House Counsel Gonzales Certifies March 11, 2004, Presidential Authorization ~~(TS//SI//NF)~~

1. March 10, 2004: Office of Legal Counsel Presses for Solicitor General to be Read into Program (U)

Goldsmith, Philbin, and Comey met in the early afternoon of March 10, 2004, to discuss the meeting at the White House the day before and how the Department should proceed. Goldsmith and Philbin reconfirmed their position to Comey that collection under [redacted] ~~(TS//STLW//SI//OC/NF)~~

Goldsmith and Philbin also recommended to Comey that Solicitor General Theodore Olson be read into the program. Goldsmith told us that Olson had been at the Department for a long time and had valuable experience and credibility. Goldsmith said that given the importance of the decisions being made at the Department concerning the program at this time, he believed it was imperative to have Olson read in. (U)

Comey agreed with Goldsmith and Philbin, and he directed Goldsmith to call Gonzales to reaffirm the Department's position on the program and also to request that Olson be read in. (U)

Goldsmith called Gonzales at 2:20 p.m. on March 10 to tell him that the Department could not support the legality of [redacted] as then being implemented under the program. Goldsmith also told Gonzales of the "urgent need" for approval to read Olson into the program. Goldsmith's notes indicate that he called Gonzales twice that day with the request to have Olson read in, but by early evening had not heard back from Gonzales. ~~(TS//STLW//SI//OC/NF)~~

2. March 10, 2004: Congressional Leaders Briefed on Situation (U)

Gonzales told us that after President Bush was advised of the results of the March 9, 2004, meeting, the President instructed Vice President Cheney on the morning of Wednesday, March 10, to call a meeting with congressional leaders to advise them of the impasse with the Justice Department. On the afternoon of March 10, at approximately 4:00 or 5:00 p.m., Gonzales and other White House and intelligence agency officials, including Vice President Cheney, Card, Hayden, McLaughlin, and Director of Central Intelligence George Tenet, convened an "emergency meeting" with Congressional leaders in the White House Situation Room. The

congressional leaders in attendance were Senate Majority and Minority Leaders Bill Frist and Tom Daschle; Senate Select Committee on Intelligence Chairman Pat Roberts and Vice Chairman Jay Rockefeller; Speaker of the House Dennis Hastert and House Minority Leader Nancy Pelosi; and House Permanent Select Committee on Intelligence Chair Porter Goss and Ranking Member Jane Harman. This congressional group was known informally as the "Gang of Eight." (U)

No officials from the Department were present at the meeting. When we asked Gonzales whether the White House had given any consideration to inviting Department officials to attend, Gonzales declined to answer on the advice of the Special Counsel to the President, who was present during Gonzales's interview with the OIG.[155] (U)

Gonzales told us that President Bush also directed him to "memorialize" the meeting, although Gonzales said he could not recall whether the President directed him to do so before or after the meeting. Gonzales did not take notes during the meeting. Rather, he said he wrote down his recollection of the meeting within a few days of Wednesday, March 10, probably, according to him, the following weekend.[156] Gonzales said that, with the exception of a single phrase discussed below, he wrote his notes in one sitting in his White House office. (U)

The notes indicate that President Bush appeared briefly at the start of the meeting to explain how important the meeting was. Vice President Cheney, who chaired the meeting, gave a general explanation of the program and indicated that the purpose of the meeting was to "discuss potential legislation to continue the program." According to Gonzales's notes, Hayden then explained the collection of "telephone content and meda data [sic]" under the program. [redacted]

---

[155] However, when Gonzales commented on a draft of this report, he stated that the Department was not invited to the meeting because the purpose of the meeting was to advise the congressional leaders that a legislative fix was necessary, not to describe or resolve the legal dispute between the Department and the White House. (U//~~FOUO~~)

[156] Gonzales's handling of his notes from this meeting later became the subject of a separate OIG misconduct investigation. The OIG found that when Gonzales became the Attorney General in 2005, he took the notes, which contained TS/SCI information relating to the Stellar Wind program, from the White House and improperly stored these notes at his residence for an indeterminate period. When he brought the notes to the Justice Department, he kept them in a safe near his office that was not cleared for storage of TS/SCI material. The OIG also determined through this investigation that Gonzales improperly stored several other TS/SCI documents in the safe near his office, many of which concerned Stellar Wind. The OIG's report, entitled "Report of Investigation Regarding Allegations of Mishandling of Classified Documents by Attorney General Alberto Gonzales," was released by the OIG on September 2, 2008, and can be found at http://www.usdoj.gov/oig/special/s0809/index.htm. ~~(S//NF)~~

[redacted]'[157] According to Gonzales's notes, the briefers then left the meeting and the remaining participants discussed the need for legislation so that the program's intelligence collection activities could continue. ~~(TS//STLW//SI//OC/NF)~~

Gonzales's notes indicate that when he was asked at the meeting why Comey was "reluctant" to sign the Authorization, Gonzales responded, [redacted] The notes do not indicate what else was discussed about the basis for the Department's concerns about the legal support for the program. ~~(TS//STLW//SI//OC/NF)~~

The notes indicate that Andrew Card stated that "it would be hard to explain if another attack occurred and we could have stopped it with this tool." Gonzales's notes then state:

- Andy asked if anyone had any reservation and no one spoke up raising an objection
- The VP said that what I am hearing is that we should go forward with the program for a period of 30-45 days and see if there was a legislative fix. ~~(TS//SI//NF)~~

The notes indicate that Vice President Cheney read aloud proposed language of new legislation. However, the notes do not describe the proposed legislation that was discussed. (U)

According to Gonzales's notes, the reactions and comments of the congressional leaders were as follows: Both Hastert and Roberts "said they now felt an obligation to use the tool," although according to the notes Hastert "kept coming back to the [redacted] Roberts said that if Comey would not certify the Authorization "he should be fired." Harman suggested that another branch of government "should have some role, checks and balances on the program" and raised the possibility of involving the FISA Court. According to the notes, Gonzales responded to Harman's suggestion by volunteering that it would be possible to have the Presiding Judge of the FISA Court "approve or develop the guidelines to protect privacy rights." The notes state that Daschle felt it would be "impossible to get [new legislation] passed

[157] Gonzales told us he was unable to recall [redacted] he was referring to in the notes, and said he did not recall whether it had to do with [redacted] (U)

without it becoming very public." Rockefeller was "concerned about privacy safeguards" and was advised of "the 39 steps followed [by the NSA] to make sure privacy concerns were addressed." According to the notes, Pelosi expressed concern about giving "total discretion" to the President and discussed the need for the proposed legislation to be periodically renewed by Congress and that it not be permanent. ~~(TS//STLW//SI//OC/NF)~~

Gonzales told us he initially left a gap in one section of the notes where he described Pelosi's comments. He stated that a day or so later, after recalling what she had said at the meeting, he filled in the gap with the following italicized language: "Pelosi said *tell DAG that everyone is comfortable* and the program should go forward."[158] (U)

3. March 10, 2004: Hospital Visit (U)

Gonzales told us that following the meeting with the congressional leaders during the afternoon of March 10, President Bush instructed him and Card to go to the George Washington University Hospital to speak to Ashcroft, who was recovering from surgery in the intensive care unit. The events that followed, which are recounted below, are based on notes from Ashcroft's FBI security detail, Goldsmith's notes, and Mueller's program log; the OIG's interviews of Gonzales, Comey, Goldsmith, Philbin, and Mueller; and Comey and Gonzales's congressional testimony.[159] (U)

At 6:20 p.m. on March 10, Card called the hospital and spoke with an agent in Ashcroft's FBI security detail, advising the agent that President Bush would be calling shortly to speak with Ashcroft. Ashcroft's wife told

---

[158] When Gonzales testified before the Senate Judiciary Committee on July 24, 2007, he essentially described the congressional leaders' reactions to the March 10, 2004, Gang of Eight briefing as he did in his handwritten notes of the briefing, stating, "The consensus in the room from the congressional leadership is that we should continue the activities, at least for now." However, after Gonzales testified, Representative Pelosi, Senator Rockefeller, and Senator Daschle issued statements to the media sharply disputing Gonzales's characterization of their statements at the March 10, 2004, briefing, and stating that there was no consensus at the meeting that the program should proceed. See "Gonzales, Senators Spar on Credibility," by Dan Eggen and Paul Kane, The Washington Post (July 25, 2007). Pelosi's office also issued a statement that she "made clear my disagreement with what the White House was asking" concerning the program. See "Gonzales Comes Under New Bipartisan Attack in Senate," by James Rowley, Bloomberg.com (July 24, 2007). We did not attempt to interview the congressional leaders and obtain their recollections as to what was said at this meeting, because this was beyond the scope of our review. (U)

[159] Comey described the events surrounding the hospital visit in testimony before the Senate Judiciary Committee on May 15, 2007. Gonzales testified about these issues before the Senate Judiciary Committee on July 24, 2007. As noted above, Attorney General Ashcroft and Card declined our request to be interviewed. Ayres, Ashcroft's Chief of Staff at the time, also declined our request for an interview. (U)

the agent that Ashcroft would not accept the call. Ten minutes later, the agent called Ashcroft's Chief of Staff David Ayres through the Justice Command Center to request that Ayres speak with Card about the President's intention to call Ashcroft. The agent conveyed to Ayres Mrs. Ashcroft's desire that no calls be made to Ashcroft for another day or two.[160] Ayres told the agent he would relay this message to Card. (U)

However, at 6:45 p.m., Card and the President called the hospital and, according to the agent's notes, "insisted on speaking [with Attorney General Ashcroft]." According to the agent's notes, Mrs. Ashcroft, rather than Attorney General Ashcroft, took the call from Card and the President. According to the agent's notes, she was informed that Gonzales and Card were coming to the hospital to see Ashcroft regarding a matter involving national security. (U)

At approximately 7:00 p.m., Ayres was advised, either by Mrs. Ashcroft or a member of the Attorney General's security detail that Gonzales and Card were on their way to the hospital. Ayres then called Comey, who at the time was being driven home by his security detail, and told Comey that Gonzales and Card were on their way to the hospital. Comey told his driver to rush him to the hospital. According to Comey, his driver activated the emergency lights on the vehicle and headed to the hospital. (U)

According to his congressional testimony, Comey then called his Chief of Staff, Chuck Rosenberg, and directed him to "get as many of my people as possible to the hospital immediately." Comey then called FBI Director Mueller, who was having dinner with his wife and daughter at a restaurant, and told him that Gonzales and Card were on their way to the hospital to see Ashcroft, and that Ashcroft was in no condition to receive guests, much less make a decision about whether to continue the program. According to Mueller's program log, Comey asked Mueller to come to the hospital to "witness [the] condition of AG." Mueller told Comey he would go to the hospital right away. (U)

At 7:05 p.m., Ayres was notified by an agent on Ashcroft's security detail that Comey was en route to the hospital. Ayres called the agent back at approximately 7:20 p.m. and told the agent that "things may get 'a little weird'" when Gonzales and Card arrived. Ayres instructed Ashcroft's security detail, which was composed of FBI agents, to give its "full support" to Comey and to follow Comey's instructions. Ayres also told the agent that the security detail should not allow the U.S. Secret Service agents who

---

[160] Ashcroft was recovering from his gallbladder surgery the prior day. He was described by those who saw him that night as being very weak and appearing heavily medicated. Philbin told us that Ashcroft was "on morphine" on the evening of March 10. (U)

would be accompanying Gonzales and Card to remove Comey from Ashcroft's room. The FBI agent told Ayres that the Attorney General's security detail would "fully back" Comey and that "this is 'our scene'." (U)

Philbin said he was leaving work that evening when he received a call from Comey, who said that Philbin needed to get to the hospital right away because Gonzales and Card were on their way there "to get Ashcroft to sign something." Comey also directed Philbin to call Goldsmith and tell him what was happening at the hospital. Philbin called Goldsmith from a taxi on his way to the hospital. Goldsmith told us he was home having dinner when he received Philbin's call telling him to go immediately to the hospital. (U)

Comey arrived at the hospital between 7:10 and 7:30 p.m.[161] In his congressional testimony, Comey said he ran up the stairs with his security detail to Ashcroft's floor, and he entered Ashcroft's room, which he described as darkened, with Ashcroft lying in bed and his wife standing by the bed. Comey said he began speaking to Ashcroft, "trying to orient him as to time and place, and try to see if he could focus on what was happening." Comey said it was not clear that Ashcroft could focus and that he "seemed pretty bad off[.]" Comey stepped out of the room into the hallway and telephoned Mueller, who was on his way to the hospital. With Mueller still on the line, Comey gave his phone to an FBI agent on Ashcroft's security detail, and according to Comey Mueller instructed the agent not to allow Comey to be removed from Ashcroft's room "under any circumstances." (U)

Goldsmith and Philbin arrived at the hospital within a few minutes of each other. Comey, Goldsmith, and Philbin met briefly in an FBI "command post" that had been set up in a room adjacent to Ashcroft's room. Moments later, word was received at the command post that Card and Gonzales had arrived at the hospital and were on their way upstairs to see Ashcroft. Philbin told us the FBI agents in the command post called down to the checkpoint at the hospital entrance to ask whether Card and Gonzales were accompanied by Secret Service agents, which Philbin said indicated concern that a "stand-off" between the FBI agents and the Secret Service agents might ensue. (U)

Comey, Goldsmith, and Philbin entered Ashcroft's room. Goldsmith described Ashcroft's appearance as "weak" and "frail," and observed that his breathing was shallow. Philbin said he was shocked by Ashcroft's appearance and said he "looked terrible." Philbin said that Ashcroft

---

[161] There is a discrepancy in the Attorney General's security detail log on the time. One agent wrote that Comey arrived at 7:10. Another agent wrote that Comey arrived at 7:30. (U)

appeared to have lost a lot of weight, was "gray in the face," and was "almost out of it" because he was on morphine. Comey stated that Ashcroft was "clearly medicated." (U)

Comey testified that he sat in an armchair by the head of Ashcroft's bed, with Goldsmith and Philbin standing behind him; Mrs. Ashcroft stood on the other side of the bed holding Ashcroft's arm. No security or medical personnel were present. (U)

Goldsmith's notes indicate that at this point Comey and the others advised Ashcroft "not to sign anything." (U)

Gonzales and Card, unaccompanied by Secret Service agents, entered Ashcroft's hospital room at 7:35 p.m., according to the FBI agent's notes.[162] The two stood across from Mrs. Ashcroft at the head of the bed, with Comey, Goldsmith, and Philbin behind them. (U)

Gonzales stated that when he entered the hospital room, Ashcroft was in the bed and his wife was "at the 11:00 position." Gonzales said to us that he was unaware that Comey, Goldsmith, and Philbin were also present in the room until Card told him this later. Gonzales told us that he could "sense" that others were in the room, but that he was not sure who, because his focus was on Ashcroft. Gonzales said he carried with him in a manila envelope the March 11, 2004, Presidential Authorization for Ashcroft to sign. (U)

According to Philbin, Gonzales first asked Ashcroft how he was feeling. Ashcroft replied, "Not well." Gonzales then said words to the effect, "You know, there's a reauthorization that has to be renewed . . . ." (U)

Goldsmith told the OIG that Gonzales next reminded Ashcroft that he had been certifying the program for the past 2 years. Comey told us that Gonzales told Ashcroft, "We have arranged for a legislative remediation; we're going to get Congress to fix it," and that more time was needed to accomplish this. Comey told us he did not know what Gonzales meant by "legislative remediation." (U)

Gonzales told us that he did not recall telling Ashcroft that a legislative remediation had been arranged, but rather may have told Ashcroft that White House officials had met with congressional leaders "to pursue a legislative fix." (U)

Comey testified to the Senate Judiciary Committee about what happened next:

---

[162] Gonzales told us he and Card arrived in Ashcroft's hospital room at 7:20. (U)

> . . . Attorney General Ashcroft then stunned me. He lifted his head off the pillow and in very strong terms expressed his view of the matter, rich in both substance and fact, which stunned me, drawn from the hourlong meeting we'd had a week earlier, and in very strong terms expressed himself, and then laid his head back down on the pillow. He seemed spent. . . . And as he laid back down, he said, "But that doesn't matter, because I'm not the Attorney General. There is the Attorney General," and he pointed to me – I was just to his left. The two men [Gonzales and Card] did not acknowledge me; they turned and walked from the room. (U)

Comey also testified that "I thought I had just witnessed an effort to take advantage of a very sick man, who did not have the powers of the Attorney General because they had been transferred to me." (U)

Philbin described to us Ashcroft's statements to Gonzales and Card in the hospital room, stating that Ashcroft "rallied and held forth for two minutes" about problems with the program as had been explained to him by Comey, and that Ashcroft agreed with Comey. Gonzales told us that he did not recall Ashcroft stating that he agreed with Comey. Goldsmith's notes indicate that Ashcroft argued in particular that NSA's collection activities exceeded the scope of the Authorizations and the OLC memoranda, stating that he was troubled by [redacted]"[163] According to Goldsmith's notes Ashcroft also said that it was "very troubling that [redacted] people in other agencies" had been read into the program, but that Ashcroft's own Chief of Staff, and until recently the Deputy Attorney General, had not been allowed to be read in. Gonzales told us he responded to Ashcroft that this was the President's decision. ~~(TS//SI//NF)~~

According to Goldsmith's notes, Ashcroft also complained that the White House had "not returned phone calls," and that the Department had been "treated badly and cut out of [the] whole affair." Ashcroft told Gonzales that he was "not prepared to sign anything." (U)

When we interviewed Gonzales about the hospital visit, he stated that these were "extraordinary circumstances," that the program had been reauthorized over the past two years, and that the sentiment of the

---

[163] As discussed in Chapter Three, Ashcroft was present for the January 31, 2002, briefing of Presiding Judge of the FISA Court Royce Lamberth about the program. According to an outline of information to be covered during that briefing, NSA Director Hayden would have explained how the program functioned operationally. Because Ashcroft did not agree to be interviewed, we were unable to determine what Ashcroft understood about the [redacted] collection prior to Philbin and Goldsmith's explanation to him of this aspect of the program in late 2003. ~~(TS//STLW//SI//OC/NF)~~

congressional leadership was that it should continue. Gonzales said he therefore felt it was very important that Ashcroft be told what was happening, adding "If I were the Attorney General I would damn sure want to know." (U)

In his July 2007 congressional testimony, Gonzales also explained the visit to the hospital by stating that it was "important that the Attorney General knew about the views and recommendations of the congressional leadership; that as a former member of Congress and as someone who had authorized these activities for over two years, that it might be important for him to hear this information. That was the reason that Mr. Card and I went to the hospital." Gonzales further testified, "We didn't know whether or not he knew of Mr. Comey's position and, if he did know, whether or not he agreed with it." Gonzales also disputed Goldsmith's account that Ashcroft stated that he was "not prepared to sign anything," and referred us to his July 2007 testimony where he stated: (U)

> My recollection, Senator [Feinstein], is – and, of course, this happened some time ago and people's recollections are going to differ. My recollection is that Mr. Ashcroft did most of the talking. At the end, my recollection is, he said, "I've been told it would be improvident for me to sign. But that doesn't matter, because I'm no longer the Attorney General." (U)

Gonzales told us that he and Card would not have gone to the hospital if they believed Ashcroft did not have the authority to certify the Authorization and told us that as soon as Ashcroft stated he no longer retained authority to act, Gonzales decided not ask Ashcroft to sign the Authorization. In his congressional testimony Gonzales stated, "Obviously there was concern about General Ashcroft's condition . . . [W]e knew, of course, that he was ill, that he'd had surgery." Gonzales also stated that "We would not have sought nor did we intend to get any approval from General Ashcroft if in fact he wasn't fully competent to make that decision." He also testified, "There's no governing legal principle that says that Mr. Ashcroft [. . .] If he decided he felt better, could decide, 'I'm feeling better and I can make this decision, and I'm going to make this decision.'"[164] (U)

The Attorney General security detail's logs indicate that Gonzales and Card left Ashcroft's room at 7:40 p.m. (U)

---

[164] Hearing before Senate Judiciary Committee, July 24, 2007. Gonzales also told us that he would not have gone to the hospital solely over the dispute concerning the scope [redacted] ~~(TS//SI//NF)~~

Moments after Gonzales and Card departed, Mueller arrived at the hospital. According to Mueller's notes, outside the hospital room Comey informed him of the exchange that had occurred in Ashcroft's room, and in particular that Ashcroft had stated that Comey was the Acting Attorney General, that "all matters" were to be taken to Comey, but that Ashcroft supported Comey's position regarding the program. Mueller's notes also state: "The AG also told [Gonzales and Card] that he was barred from obtaining the advice he needed on the program by the strict compartmentalization rules of the [White House]." (U)

Mueller's notes indicate that Comey asked Mueller to witness Ashcroft's condition, and requested Mueller to inform the FBI security detail that no visitors, other than family, be allowed to see Ashcroft without Mueller's consent. Both Mueller's notes and the security detail log indicate that Mueller instructed the detail that under no circumstances was anyone to be allowed into Ashcroft's room without express approval from either Mrs. Ashcroft or Mueller. (U)

At approximately 8:00 p.m. Mueller went into Ashcroft's room for 5 to 10 minutes. Mueller wrote in his program log: "AG in chair; is feeble, barely articulate, clearly stressed." (U)

4. March 10, 2004: Olson is Read into the Program (U)

According to Comey's congressional testimony, while he was speaking with Mueller prior to Mueller's departure from the hospital, an FBI agent interrupted, stating that Comey had an urgent telephone call from Card. Comey testified that he then spoke with Card, who was very upset and demanded that Comey come to the White House immediately. Comey testified that he told Card that based on the conduct Comey had just witnessed at the hospital, he would not meet with Card without a witness present. Comey testified that Card replied, "What conduct? We were just there to wish him well." Comey reiterated his condition that he would only meet Card with a witness present, and that he intended the witness to be Solicitor General Olson. Comey testified that until he could "connect" with Olson, he was not going to meet with Card. Card asked if Comey was refusing to come to the White House, and Comey responded that he was not refusing and would be there, but that he had to go back to the Justice Department first. (U)

Comey and the other Department officials left the hospital at 8:10 p.m. Philbin stated that he returned to the Department with Comey in Comey's vehicle, and that the emergency lights were again activated. Goldsmith also left the hospital and went to the Department. At the Department Comey, Goldsmith, and Philbin were joined by Olson, who had come to the Justice Department after being contacted at a dinner party.

Comey told us that he believed there was an urgent need to have Olson read into the program because he was confident Olson would agree with Comey and the others that Yoo's legal analysis was flawed and that Olson would be a strong ally in the matter because of Olson's respected intellect and credibility. (U)

During this meeting at the Justice Department, a call came from Vice President Cheney for Olson, which Olson took on a secure line in Comey's office while Comey waited outside. Comey told us he believes Vice President Cheney effectively read Olson into the program during that conversation. (U)

Comey and Olson then went to the White House at about 11:00 p.m., and met with Gonzales and Card that evening. Comey testified that Card would not allow Olson to enter his office. Comey relented and spoke to Card alone for about 15 minutes. At that point, Gonzales arrived and brought Olson into the room. According to Comey, he communicated the Department's views on the dispute and that the dispute was not resolved in this discussion. Comey stated that Card was concerned that he had heard reports that there was to be a large number of resignations at the Department. (U)

Gonzales told us that he recalled that Comey met first with him and Card while Olson waited outside the office, and that Olson joined them shortly thereafter. Gonzales said that little more was achieved than a general acknowledgement that a "situation" continued to exist because of the disagreement between the Department and the White House regarding the program.[165] (U)

5. March 11, 2004: Goldsmith Proposes Compromise Solution (U)

According to a memorandum to the file drafted by Goldsmith, he met with Gonzales at 6:30 a.m. the next morning, March 11, 2004, at the White House to discuss a proposal under which the Department could support

---

[165] Comey stated that Olson did not become deeply involved in analyzing the Stellar Wind program in the days that followed because he was preparing for a major argument before the Supreme Court. Comey told us that Deputy Solicitor General Paul Clement was read into the program on March 12, 2004, and reviewed all of the OLC memoranda that weekend. Comey said Clement agreed with Goldsmith and Philbin's analysis "one hundred percent" and later worked with the OLC on drafting a new memorandum on the legality of the program, which is discussed below. However, Bradbury told us that Comey's characterization of Clement's view of the analysis was exaggerated. Bradbury told us that Clement had remarked to him after these events transpired that Goldsmith and Philbin's analysis "sounded reasonable to me at the time," and that Clement's view of the analysis was based only on a limited review of it. ~~(TS//SI//NF)~~

certification of the program. Goldsmith's proposal had three conditions.

[redacted] ~~(TS//STLW//SI//OC/NF)~~

Goldsmith told us that he did not specifically recall this meeting. Gonzales told us that he recalled conveying to Goldsmith and Philbin at some point during this day that the President had decided he had the constitutional authority to continue the program. Gonzales said he also expressed to Department officials the sentiment that the Department should continue seeking a way to "get comfortable" with the President's decision. (U)

6. March 11, 2004: White House Asserts that Comey's Status as Acting Attorney General was Unclear (U)

Goldsmith told the OIG that later during the morning of March 11, 2004, he received a call from Deputy White House Counsel David Leitch. Goldsmith said Leitch was "yelling and screaming" about the White House not being informed that Comey was the Acting Attorney General. Goldsmith told the OIG that Leitch made two specific complaints. First, Leitch claimed that the White House had never received a determination from OLC on Comey's assumption of Ashcroft's powers and duties. Goldsmith told us that to rebut this charge, OLC Deputy Assistant Attorney General Edward Whelan was sent to the Justice Command Center to retrieve from a waste basket the facsimile transmittal confirmation sheet from the March 5, 2004, memorandum Goldsmith had sent to Gonzales entitled "Determination that Attorney General is absent or disabled." This confirmation sheet subsequently was sent to Leitch.[166] (U)

---

[166] In a March 12, 2004, e-mail to Ayres, Comey, Goldsmith, Philbin, and others (including a copy to Gonzales), Leitch offered a "clarification," asserting that the White House had in fact received the Goldsmith memoranda of March 5, as well as the

(Cont'd.)

Leitch's second claim was that the OLC memorandum was ambiguous because it did not specify whether the Attorney General was determined to be "absent" or "disabled," a difference for purposes of the Attorney General's authority. According to Goldsmith, if the Attorney General was "absent," the Deputy Attorney General could act as the Attorney General, although the Attorney General would retain his authority and technically could overrule the Deputy. If the Attorney General was "disabled," the Attorney General was divested of all authority. Goldsmith said he responded to Leitch by noting the inconsistency of the White House making this second claim because, according to Leitch, it had not received Goldsmith's memorandum in the first instance. (U)

Goldsmith said he also told Leitch to "lay off" the complaints, but that Leitch did not. Goldsmith said he therefore reluctantly sent a detailed e-mail to Leitch on March 11 to support the Department's contention that it had properly informed the White House of Ashcroft's status. Goldsmith stated that in the e-mail he also made the point that his conversation with Gonzales on March 9, 2004 (discussed above) was premised on Gonzales's knowledge that Ashcroft was ill and that Comey needed to authorize a "30-day bridge" until Ashcroft was well enough to sign the Authorizations again.[167] (U)

Gonzales told us that he had no recollection of having seen OLC's March 5, 2004, memorandum entitled "Determination that Attorney General is absent or disabled." As described above, Gonzales stated that he and Card would not have gone to the hospital if they believed Ashcroft did not have the authority to certify the Authorization as to form and legality. Gonzales also said that while he believed Comey would be making the decision to recertify the program, this did not mean that Ashcroft had relinquished his authority or had been "recused" from making the decision. Gonzales said he believed that Ashcroft retained the authority if he was competent to exercise it and was inclined to do so.[168] ~~(TS//SI//NF)~~

---

memorandum from Comey's Chief of Staff Chuck Rosenberg memorializing Comey's decision that the Attorney General was "absent or disabled" within the meaning of 28 U.S.C. § 508(a). Leitch's clarification stated that the Rosenberg memorandum had been in draft form. (U)

[167] The OIG searched for but was unable to find this e-mail from Goldsmith to Leitch. (U)

[168] During his July 24, 2007, testimony before the Senate Judiciary Committee, however, Gonzales stated that he thought there had been newspaper accounts of Comey's assumption of the Attorney General's duties and stated that "the fact that Mr. Comey was the acting Attorney General is probably something that I knew of." Gonzales testified that he was aware that Ashcroft was ill and had undergone surgery, but Gonzales stated that Ashcroft "could always reclaim" his authority. (U)

7. March 11, 2004: Gonzales Certifies Presidential Authorization as to Form and Legality ~~(TS//SI//NF)~~

On the morning of March 11, 2004, with the Presidential Authorization set to expire, President Bush signed a new Authorization.[169] In a departure from the past practice of having the Attorney General certify the Authorization as to form and legality, the March 11 Authorization was certified by White House Counsel Gonzales. The March 11 Authorization also differed markedly from prior Authorizations in three other respects. ~~(TS//STLW//SI//OC/NF)~~

The first significant difference between the March 11, 2004, Presidential Authorization and prior Authorizations was the President's explicit assertion that the exercise of his Article II Commander-in-Chief authority [redacted]

As discussed above, FISA and the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2521 (generally referred to as Title III) are by their terms the "exclusive means by which electronic surveillance, as defined in [FISA], and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f). This new language was based on the same legal rationale Yoo first advanced in support of the Stellar Wind program – that FISA cannot be read to infringe upon the President's Commander-in-Chief authority under Article II of the Constitution during wartime. ~~(TS//STLW//SI//OC/NF)~~

[redacted] Steven Bradbury told the OIG that he believed the language was included in the March 11 Authorization as a way of indicating that the President did not agree with Goldsmith and Philbin's analysis, and to protect those who had been implementing the program under the prior OLC opinions. ~~(TS//SI//NF)~~

Second, [redacted]

[169] The March 11, 2004, Presidential Authorization stated that it would expire on May 6, 2004. ~~(TS//SI//NF)~~

[redacted]

[redacted]

170 [redacted] (TS//SI//NF)

[redacted]

According to Comey and Philbin, this new language was Addington's "fix."[172] Philbin said he believed the new language was "sufficient" to address the Department's concern that the Authorizations did not adequately describe the [redacted] being carried out by the NSA, although he believed the new language was "cumbersome." [redacted]

~~(TS//STLW//SI//OC/NF)~~

In his OIG interview, Gonzales declined to explain the significance of this new language, based on an assertion from the Special Counsel to the President that his answer would reveal internal White House deliberations [redacted]

~~(TS//STLW//SI//OC/NF)~~

[171] [redacted]

~~(TS//STLW//SI//OC/NF)~~

[172] Hayden and Philbin both told the OIG that Addington drafted the Presidential Authorizations. In his OIG interview, we asked Gonzales who drafted the March 11, 2004, Authorization. On the advice of the Special Counsel to the President, Gonzales declined to answer. ~~(TS//SI//NF)~~

The March 11 Presidential Authorization did not [redacted] (~~TS//STLW//SI//OC/NF~~)

The third significant departure from prior Authorizations was the inclusion of a statement that [redacted] Id. at para. 10. (~~TS//STLW//SI//OC/NF~~)

[redacted]

[redacted]

[redacted]

173

[redacted]

However, Gonzales told us that he found it "hard to believe" that no one at the Department understood that the NSA [redacted] Gonzales said he was aware that Philbin had been to the NSA several times and had met with NSA officials to gain an understanding of how the program was actually implemented. (~~TS//STLW//SI//OC/NF~~)

[redacted]

We asked Gonzales why he signed the March 11, 2004, Presidential Authorization even though the Department could not support it. On the advice of the Special Counsel to the President, Gonzales declined to answer. However, Gonzales stated that the White House Counsel, like OLC, provides legal advice to the President and that his signature on the Authorization simply represented his advice as to its form and legality. ~~(TS//SI//NF)~~

NSA Director Hayden told us that Addington asked him whether the NSA would be willing to continue the Stellar Wind program without the Justice Department's certification of the Presidential Authorization. Hayden said this was a "tough question" and that he consulted with his leadership team at the NSA before making a decision. Hayden said that three considerations persuaded him to continue the program. First, the congressional members briefed on the situation on March 10, 2004, were supportive of continuing the program without Comey's certification. Second, the program had been operating for the previous two and a half years with Department approval. Third, the NSA General Counsel's office told him the program was legal. Hayden said he was unsure whether proceeding without the Department's certification was a sustainable approach, but that he was comfortable doing so when the issue arose in March 2004. ~~(TS//SI//NF)~~

B. Department and FBI Officials React to Issuance of March 11, 2004, Authorization ~~(TS//SI//NF)~~

Several Department and FBI leadership officials considered resigning after the Presidential Authorization was signed despite the Deputy Attorney General's refusal to certify the program based on the Department's determination that certain activities it authorized were without adequate legal support. Many of the Department, FBI, and White House officials we interviewed characterized the events immediately surrounding the issuance

---

[174] In a closed session of the Senate Select Committee on Intelligence on June 26, 2007, Comey described his belief regarding the new language, stating, "[T]here were some additions to the text that were an effort by someone to try and fix the record in some respect." (U//~~FOUO~~)

of the March 11, 2004, Presidential Authorization in dramatic, sharp terms. Several of the Department witnesses described the impasse as a "crisis" and described a sense of distrust and anger that permeated their relations with White House officials during this period. In a letter of resignation that Comey wrote but did not send, he described this period as an "apocalyptic situation." ~~(TS//SI//NF)~~

In this section, we describe the reactions of Department, FBI, and White House officials to the White House decision to continue the program without the support of the Justice Department. (U)

1. Initial Responses of Department and FBI Officials (U)

White House Chief of Staff Card informed Comey by telephone on the morning of March 11, 2004, that the President had signed the new Authorization that morning. At approximately noon, Gonzales called Goldsmith to inform him that the President, in issuing the Authorization, had made an interpretation of law concerning his authorities and that the Department should not act in contradiction of his determinations. Goldsmith took notes on the call. According to his notes, Goldsmith asked Gonzales, "What were those determinations?" and Gonzales responded that he would let Goldsmith know. ~~(TS//SI//NF)~~

Later that day, Gonzales called Goldsmith again and told him that OLC should continue working on its legal analysis of the program. In a third call that day, however, Gonzales directed Goldsmith to suspend work on the legal analysis and to decline a request from the CIA General Counsel to review a draft of the new OLC memorandum. ~~(TS//SI//NF)~~

Goldsmith followed up this series of calls with a letter to Gonzales seeking clarification on Gonzales's instructions. Goldsmith wrote that he interpreted the March 11, 2004, Authorization signed by the President to mean that "the President has determined the legality of [the program] in all respects based upon the advice and analysis of your office, and that officers of the Department of Justice should refrain from calling into question the legality of [the program], or from undertaking further legal analysis of it." In the letter Goldsmith recounted how Gonzales had then called him to advise that OLC should continue its legal analysis of the program, adding, "I am now uncertain about your direction based on the President's exercise of his authority." Goldsmith concluded his letter by reiterating OLC's position that its existing legal memoranda "should not be relied upon in support for the entire program." Goldsmith described the document he wrote as a "for the record" letter.[175] As described below, Goldsmith and Philbin delivered

[175] Goldsmith said he discussed a draft of the letter with Comey, Rosenberg, Ayres, Olson, and others and edited it based on their suggestions. (U)

this letter to Gonzales at his residence at approximately 11:00 p.m. that night. ~~(TS//SI//NF)~~

At noon on March 11, 2004, Director Mueller met with Card at the White House. According to Mueller's program log, Card summoned Mueller to his office to bring Mueller up to date on the events of the preceding 24 hours. Card recounted for Mueller the briefing of the congressional leaders the prior afternoon and the President's issuance of the new Authorization without the Department's approval. In addition, Card told Mueller that if no "legislative fix" could be found by May 6, 2004, when the current Authorization was set to expire, the program would be discontinued. ~~(TS//SI//NF)~~

According to Mueller's notes, Card acknowledged to Mueller that President Bush had sent him and Gonzales to the hospital to seek Ashcroft's certification for the March 11, 2004, Authorization, but that Ashcroft had said he was too ill to make the determination and that Comey was the Acting Attorney General. Mueller wrote in his program log that he told Card that the failure to have Department of Justice representation at the congressional briefing and the attempt to have Ashcroft certify the Authorization without going through Comey "gave the strong perception that the [White House] was trying to do an end run around the Acting [Attorney General] whom they knew to have serious concerns as to the legality of portions of the program." Card responded that he and Gonzales were unaware at the time of the hospital visit that Comey was the Acting Attorney General, and that they had only been following the directions of the President. ~~(TS//SI//NF)~~

Mueller reminded Card that Mueller had told Vice President Cheney during their March 9, 2004, noon meeting that Mueller could have problems with the FBI's continued involvement in the program if the White House issued an Authorization without the Department's approval. Card said he understood Mueller's concern and told him to stop by Gonzales's office to pick up a copy of the March 11, 2004, Authorization, which Mueller did. ~~(TS//SI//NF)~~

Mueller met with Comey at 1:15 p.m. to review the Authorization, and he left a copy of it with Comey. During this meeting, Mueller told Comey he would be submitting a letter to Comey requesting advice on the legality of the FBI's continued participation in the program.[176] ~~(TS//SI//NF)~~

[176] According to the Mueller's program log, Gonzales called Mueller at 2:50 p.m. to tell him to "assure security of copy of President's order." (U)

Later that day, Mueller sent Comey a memorandum, prepared by FBI General Counsel Valerie Caproni and an FBI Deputy General Counsel, seeking guidance on how the FBI should proceed in light of recent developments. The memorandum asked whether FBI agents detailed to the NSA to work on Stellar Wind should be recalled; whether the FBI should continue to receive and investigate tips based on [redacted] and whether [redacted] ~~(TS//STLW//SI//OC/NF)~~

Office of Intelligence Policy and Review (OIPR) Counsel James Baker also expressed his concern about the White House's action. On the evening of March 11, 2004, he drafted a memorandum to Comey containing what he later described as a series of "loaded questions" concerning whether it was "lawful and ethical" for OIPR to continue filing applications with the FISA Court under the circumstances.[177] ~~(TS//SI//NF)~~

Goldsmith and Philbin called Gonzales late in the evening of March 11 to ask if they could visit him at his residence to deliver the letter Goldsmith had written earlier in the day. As described above, Goldsmith sought to make a record of his earlier conversations with Gonzales in which Goldsmith believed Gonzales had conveyed conflicting instructions regarding how OLC should proceed in light of the President's issuance of the March 11 Authorization. ~~(TS//SI//NF)~~

Gonzales told us that Goldsmith drafted the letter because Goldsmith was "confused" about whether OLC should continue working on its legal analysis of the program. Gonzales said he recalled that Goldsmith and Philbin were "somber" during the meeting at his house. Gonzales said that he told them that the President had decided to go forward with the program, but that they should continue working to resolve the outstanding legal questions they had and try to find a solution. He said he tried to convey to them his confidence that everyone would "get through this." ~~(TS//SI//NF)~~

Goldsmith and Philbin told us that Gonzales was very cordial during the meeting and expressed regret for having gone to Ashcroft's hospital room that evening. Philbin stated that initially he believed that Gonzales had instructed him and Goldsmith "not to do our job, not to determine what the law is," but that it became evident to him that Gonzales "wanted to do the legally right thing." Goldsmith also stated that as a general proposition

---

[177] These issues are described in Section II C of this chapter in connection with the Department's meetings with FISA Court Presiding Judge Kollar-Kotelly to discuss the use in FISA applications of information derived from [redacted] collected under the program following the March 11, 2004, Presidential Authorization and its subsequent modifications. ~~(TS//STLW//SI//OC/NF)~~

he encountered more "pushback" from Addington than from Gonzales, and that Gonzales "wanted to do the right thing." ~~(TS//SI//NF)~~

2. Department and FBI Officials Consider Resigning (U)

Comey told us he drafted a letter of resignation shortly after the incident in Ashcroft's hospital room on March 10. Comey said he drafted the letter because he believed it was impossible for him to remain with the Department if the President would do something the Department said was not legally supportable.[178] (U)

Comey also testified that Ashcroft's Chief of Staff David Ayres believed Ashcroft also was likely to resign and urged Comey to wait until Ashcroft was well enough to resign with him. In written responses to Senator Charles Schumer following his testimony, Comey wrote that he believed the following individuals also were prepared to resign: Goldsmith, Philbin, Chuck Rosenberg, Daniel Levin, James Baker, David Ayres, Deputy Chief of Staff to the Attorney General David Israelite, and Director Mueller. Comey also responded to the question that he believed that "a large portion" of his staff also would have resigned if he had. (U)

Goldsmith told us he was "completely disgusted" by his recent meetings with White House officials in connection with the Stellar Wind program and that he drafted a resignation letter at around the same time as Comey. The OIG obtained a handwritten list Goldsmith had compiled as these events were taking place to memorialize his grievances with the White House's actions during this period. The list includes:

- the "[s]hoddiness of the whole thing," which Goldsmith told us referred to his belief that both the process by which the program was implemented and the substantive analysis underpinning it represented the extreme opposite of how to manage a program as important as the White House claimed Stellar Wind to be;

---

[178] The letter was addressed to President Bush. Also, at 5:46 p.m. on the evening of March 11, 2004, Comey sent an e-mail to two Department colleagues stating in part:

> I have been through the roughest patch of my professional life in the last 24 hours. You would not believe what has gone on . . . . I am hugely upset about the conduct of certain members of the executive branch. But I am also hugely proud of the Department of Justice, including SG, Associate AG, OLC, Ayres, my staff, the AG, and even Mrs. Ashcroft. I believe this has been our finest hour, although it is not over yet. . . . I suspect I will either be fired by the President or quit, but I will have done the right thing for my country. (U)

- "[o]ver-secrecy," both in terms of not reading in attorneys at the Justice Department and other agencies, and not keeping Congress informed;
- the hospital incident, which Goldsmith described as "shameful"; "[d]isregard of law" on the part of the White House (a reference Goldsmith did not expand upon with more specificity during his interview with the OIG); and
- the White House's claim that a legislative fix could be achieved, which Goldsmith regarded as "irresponsible" because he believed at the time that a legislative remedy was not a viable option. ~~(TS//SI//NF)~~

Goldsmith described three additional items on the list in particular as "false representations" by the White House:

- "[l]ies re shutting down," referring to the White House's assurances to Goldsmith on several occasions that it would shut down the program if the Office of Legal Counsel could not find legal support for it;
- "[l]ies re telling [the President] of problem," referring to representations that the President had been kept informed of the Department's concerns about the program; and
- assertions by White House officials that they "[d]idn't know AG was incapacitated". ~~(TS//SI//NF)~~

Goldsmith stated that on Thursday, March 11, Ayres asked him not to resign because the Attorney General should have the chance to do so first once he had fully recovered from his surgery. Goldsmith said he was still "on the fence" the following Monday or Tuesday about resigning and that there was great concern that his and other resignations would "spark a panic" that might lead to the program being revealed publicly.[179] (U)

Philbin told us that there was an "eerie silence" at the Department on March 11 as he and others awaited word from the White House on the fate of the program. Philbin said he and others believed they would have to resign. Philbin said his primary concern was that the White House planned to go forward with the Presidential Authorization and continue the program

[179] Goldsmith ultimately tendered his resignation in June 2004, effective July 30, 2004. Goldsmith told us he resigned in part because he did not believe he could be an effective head of the Office of Legal Counsel after his "unprecedented" withdrawal of several legal memoranda, including those drafted by Yoo. Goldsmith added that he also resigned because he was "exhausted" from his work in OLC and had recently been offered a teaching position at Harvard Law School. (U)

despite the flaws that the Office of Legal Counsel had identified in its legal analysis. Philbin said he was "absolutely serious" about resigning, adding, "[If] they're going to try to strong-arm the guy on morphine, what else are they going to do?" ~~(TS//SI//NF)~~

Baker told us that he also considered resigning after the President signed the Authorization but ultimately decided to remain in his position, in part because of his fear that if the White House was willing to tolerate mass resignations of senior government officials rather than revise the Stellar Wind program, "I don't know what this means in terms of the rule of law in this country." Baker also stated that he knew he had certain protections from removal for a period of time because he was a career official and that he wanted to remain as Chief of OIPR to protect the government's relationship with the FISA Court and to protect the attorneys in his office. ~~(TS//SI//NF)~~

Levin said he was willing to resign over the matter, and he gave a signed resignation letter to Comey to be used by him "however [he] felt appropriate." Levin said he did so "if it would help to get the White House to change its mind." Levin said that even though he was not certain he shared Goldsmith's view that the [redacted] was legally without support, he thought the White House's conduct during the incident at the hospital had been "outrageous" and he was willing to resign on that basis alone. ~~(TS//STLW//SI//OC/NF)~~

FBI General Counsel Caproni told us that she also was prepared to resign. She said that the FBI's primary concern regarding the impasse between the Department and the White House over the program was not with issues of privacy and civil liberties, but rather with "the rule of law." ~~(TS//SI//NF)~~

At approximately 1:30 a.m. on March 12, 2004, Mueller drafted by hand a letter stating, in part: "[A]fter reviewing the plain language of the FISA statute, and the order issued yesterday by the President . . . and in the absence of further clarification of the legality of the program from the Attorney General, I am forced to withdraw the FBI from participation in the program. Further, should the President order the continuation of the FBI's participation in the program, and in the absence of further legal advice from the AG, I would be constrained to resign as Director of the FBI." Mueller told us he planned on having the letter typed and then tendering it, along with his March 11, 2004, memorandum to Comey, but that based on subsequent events his resignation was not necessary. ~~(TS//SI//NF)~~

3. Comey and Mueller Meet with President Bush (U)

On the morning of March 12, 2004, Comey and Mueller went to the White House to attend the regular daily threat briefing with the President in the Oval Office. Comey said that following the briefing President Bush called him into the President's private study for an "unscheduled meeting." (U)

Comey told us that President Bush said to him, "You look burdened." Comey told the President that he did feel burdened, to which the President responded, "Let me lift that burden from you." Comey told the President that he felt as if he were standing on railroad tracks with a train coming toward him to run over his career and "I can't get off the tracks." (U)

Comey said he then explained to the President the three baskets of Stellar Wind collection and the issues and problems associated with each. President Bush responded with words to the effect, "You whipped this on me" all of a sudden, that he was hearing about these problems at the last minute, and that the President not being told of these developments regarding the program was "not fair to the American people." Comey responded that the President's staff had been advised of these issues "for weeks," and that the President was being "poorly served" and "misled" by his advisors. Comey also said to the President, "The American people are going to freak when they hear what collection is going on." President Bush responded, "That's for me to worry about." ~~(TS//STLW//SI//OC/NF)~~

According to Comey, the President said that he just needed until May 6 (the date of the next Authorization), and that if he could not get Congress to fix FISA by then he would shut down the program. The President emphasized the importance of the program and that it "saves lives." Comey told the President that while he understood the President's position he still could not agree to certify the program. Comey said he then quoted Martin Luther to the President: "Here I stand, I can do no other." At the end of the conversation, Comey told the President, "You should know that Bob Mueller is going to resign this morning." The President thanked Comey for telling him that and said he would speak with Mueller next. ~~(TS//STLW//SI//OC/NF)~~

Comey said his conversation with the President lasted approximately 15 minutes. Following the conversation, Comey went to Mueller, who was waiting in the West Wing, and started discussing his meeting with the

President. Word was then sent to Mueller through a Secret Service agent that the President wanted to meet with him.[180] (U)

Mueller later made notes in his program log about his meeting with President Bush. According to his notes, the President told Mueller that he was "tremendously concerned" about another terrorist attack and that he had been informed that the Stellar Wind program was essential to protecting against another attack. The President cited an ongoing investigation [redacted] The President said he believed that he would be "justly held accountable" if he did not do everything possible to prevent another attack. The President explained to Mueller that for these reasons he had authorized the continuation of the program even without the concurrence of the Attorney General as to the legality of "various aspects of the program." ~~(TS//STLW//SI//OC/NF)~~

According to the notes, the President told Mueller that the congressional leadership had been briefed on the President's action to extend the program and was "understanding and supportive of the President's position." The President also told Mueller that he had urged Comey to agree to extend the program until May 6 and that he hoped for a legislative fix by that time, but that if no legislative solution could be found and the legality of the program was still in question by that time, he "would shut it down." ~~(TS//SI//NF)~~

According to Mueller's notes, Mueller told the President of his concerns regarding the FBI's continued participation in the program without an opinion from the Attorney General as to its legality, and that he was considering resigning if the FBI were directed to continue to participate without the concurrence of the Attorney General. The President responded that he "wished to relieve any burden [Mueller] may be laboring under" and that he did not want Mueller to resign. Mueller said he explained to the President that he had an "independent obligation to the FBI and to the Justice Department to assure the legality of actions we undertook, and that a presidential order alone could not do that." ~~(TS//SI//NF)~~

---

[180] At this point (9:27 a.m.), Comey sent an e-mail from his Blackberry to Goldsmith, Philbin, Ayres, Levin, and others, stating:

> President just took me into his private office for 15 minute one on one talk. Told him he was being misled and poorly served. We had a very full and frank exchange. Don't know that either of us can see a way out. He promised that he would shut down 5/6 if Congress didn't fix FISA. Told him Mueller was about to resign. He just pulled Bob into his office. ~~(TS//SI//NF)~~

According to Mueller's notes, the President expressed understanding for Mueller's position and asked what needed to be done to address Mueller's concerns. Mueller responded that Comey, the Office of Legal Counsel, the CIA, and the NSA "needed to sit down immediately" and assess the legal status of the program in light of OLC's doubts about the existing legal rationale and the March 11, 2004, Authorization. Mueller wrote:

> The President questioned me closely on the impact on national security from discontinuing elements of the program. [redacted]

According to Mueller's notes, the President then directed Mueller to meet with Comey and other principals to address the legal concerns so that the FBI could continue participating in the program "as appropriate under the law." ~~(TS//SI//NF)~~

Mueller told us he met with Comey an hour later to begin coordinating that effort. At 4:50 p.m. that afternoon, Mueller called Gonzales to request that additional Department lawyers be read into the program.[181] Mueller told us that this request originated with Comey and that Mueller was merely acting as an "intermediary." (U)

The President's direction to Mueller to meet with Comey and other principals to address the legal concerns averted the mass resignations at the Department and the FBI. According to Comey and other Department officials, the White House's decision to seek a legal solution and allow more attorneys to be read into the program was a significant step toward resolving the dispute, and in the words of one Department official provided a way of "stepping back from the brink." As we describe below, these Department officials still faced the challenge of finding a legal and operational remedy for the program that would address the concerns of the White House, the NSA, and Department. ~~(TS//SI//NF)~~

4. Comey Directs Continued Cooperation with NSA (U)

On the morning of March 12, 2004, Comey decided not to direct OIPR and the FBI to cease cooperating with the NSA in conjunction with the program. Comey's decision is documented in a 1-page memorandum from

[181] At least three additional Department attorneys were read into the program on March 12, 2004, including OIPR Acting Deputy Counsel for Intelligence Operations Peggy Skelly-Nolen and two OLC attorneys. (U)

Goldsmith to Comey in which Goldsmith explained why Comey's action was legal. ~~(S//NF)~~

In his memorandum, Goldsmith stated that the President, as Commander-in-Chief and Chief Executive with the constitutional duty to "take care that the laws are faithfully executed," made a determination that Stellar Wind, as practiced, was lawful. Goldsmith concluded that this determination was binding on the entire Executive Branch, including Comey in his exercise of the powers of the Attorney General.[182] ~~(TS//SI//NF)~~

[redacted]

5. Department Conducts Additional Legal Analysis (U)

On March 12, 2004, an interagency working group was convened to continue the legal analysis of the program. In accordance with the President's directive to Mueller, officials from the FBI, NSA, and the CIA were brought into the process, although the OLC maintained the lead role. The working group included Deputy Solicitor General Clement, Baker, FBI General Counsel Caproni, Mueller, and several attorneys from OLC. Comey said CIA Director Tenet and his Deputy, McLaughlin, may have had limited participation as well. ~~(TS//STLW//SI//OC/NF)~~

On March 13, Mueller asked NSA Director Hayden to assist FBI General Counsel Caproni in assessing the value of the Stellar Wind program. Mueller said he wanted Caproni to become more familiar with the program and to understand how the FBI's view of the value of the program

[182] Goldsmith told us his determination that the entire Executive Branch was bound by the President's interpretation of law was based on his discussions with several other Justice Department attorneys, as well as on long-standing OLC precedent. (U)

compared with that of the NSA.[183] Mueller said that Hayden provided slides highlighting cases in which the NSA believed Stellar Wind-derived information proved useful. ~~(S//NF)~~

Caproni told us that during this March 2004 period she and two other FBI officials made an effort to determine what value the FBI was getting from Stellar Wind-derived information. She explained that it was difficult to assess the value of the program during its early stages because FBI field offices at that time were not required to report back to FBI Headquarters with information about how information from the NSA program had been used.[184] ~~(S//NF)~~

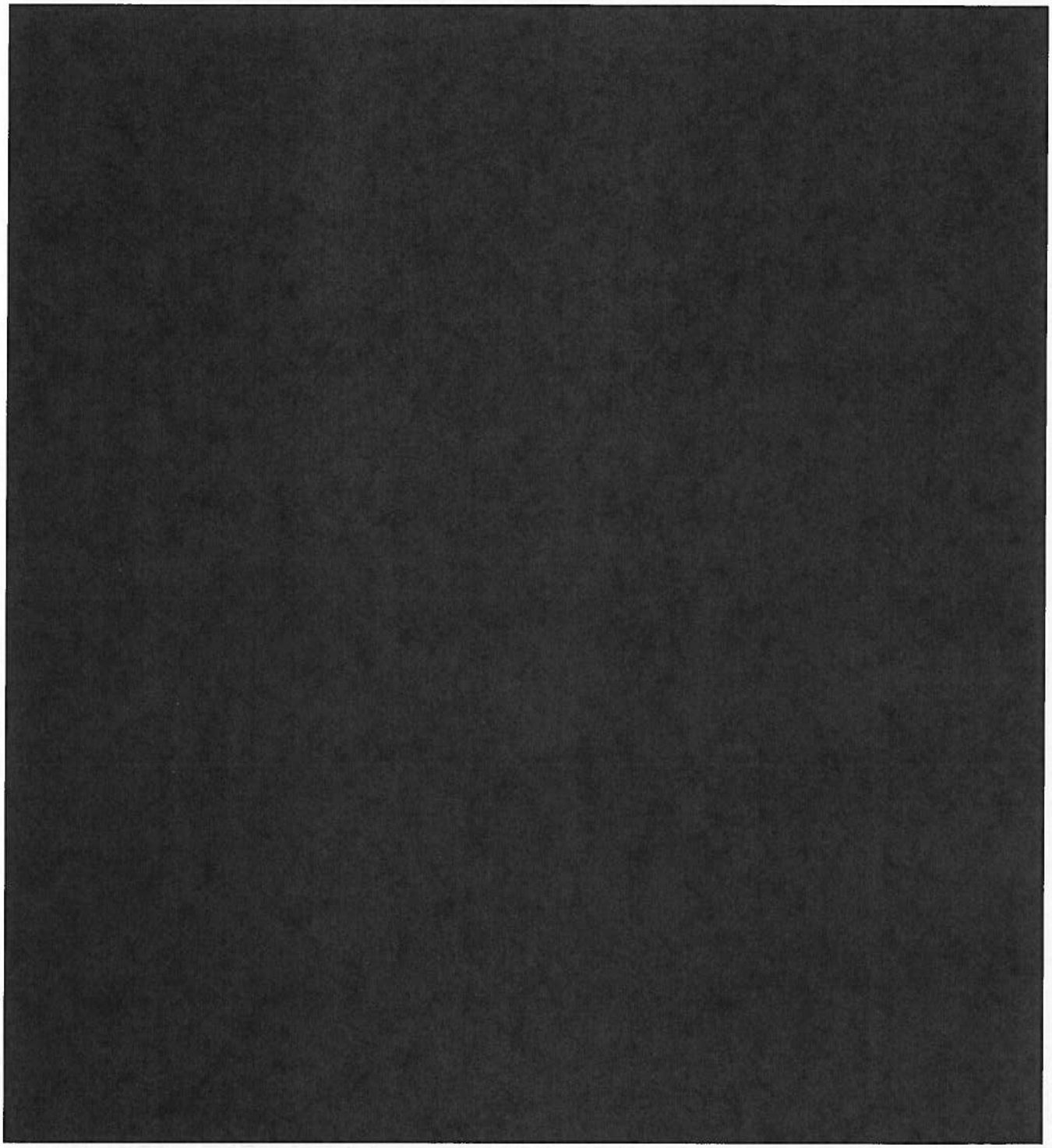
On the afternoon of Sunday, March 14, 2004, the Department convened a large meeting in the Justice Command Center to review OLC's analysis on the legality of the program. Mueller, Comey, Goldsmith, Philbin, Baker, CIA General Counsel Muller, Caproni, Tenet, Hayden, Olson, Clement, and several NSA lawyers attended the meeting. ~~(TS//SI//NF)~~

Prior to the meeting, Goldsmith and Philbin prepared a detailed outline of OLC's current analysis, which Goldsmith described to us as his "most honest take" of the legal issues at that time. Goldsmith said he distributed the outline to meeting participants and used it to walk the group through the analysis. (U)

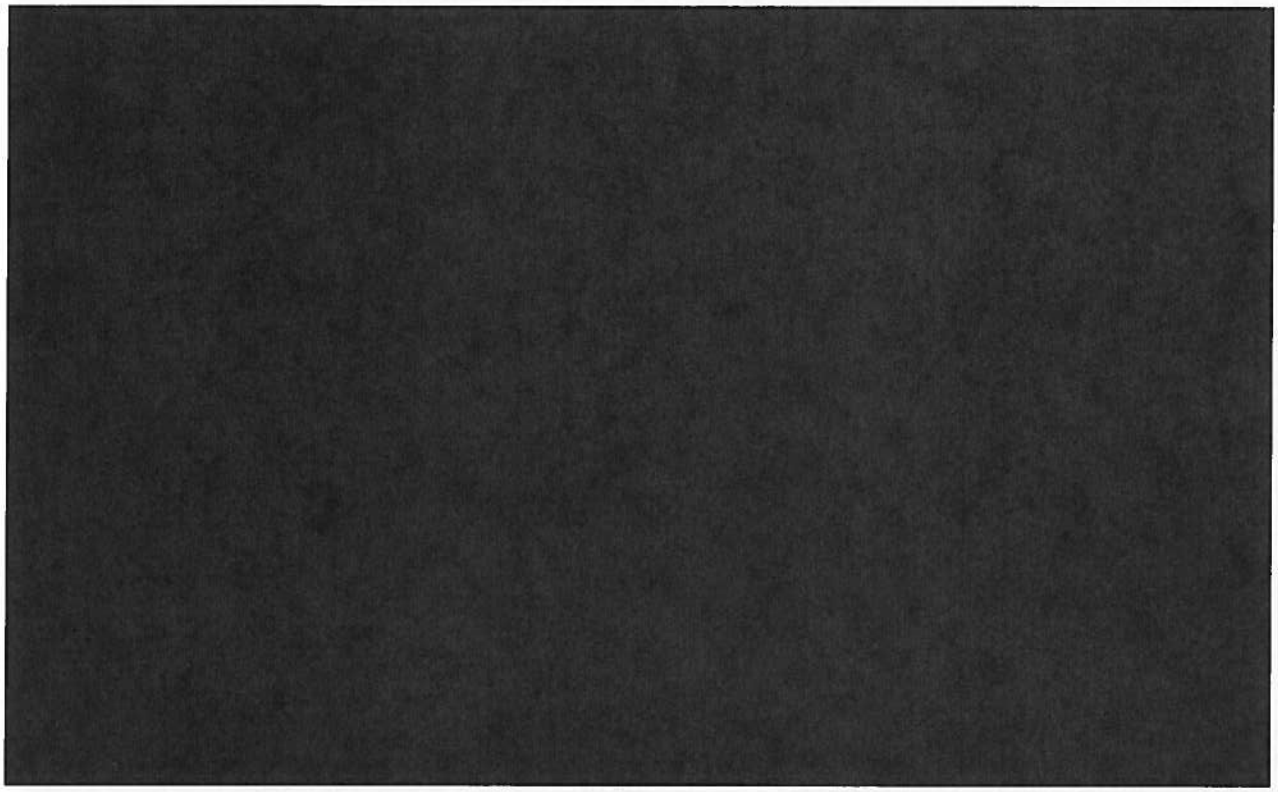
The outline highlights the evolution of OLC's analysis. [redacted]

[183] Caproni had been appointed the FBI General Counsel in August 2003 and was read into the Stellar Wind program in September or October 2003. She told us she did not give much thought to the program at the time because OLC had determined that it was legal. She stated that in 2004 she learned that OLC was re-examining Yoo's legal analysis and had concerns with it. She told us she later spoke with Philbin, who confirmed to her that he and Goldsmith had problems with the legal support for the program and that he was frustrated because the program was so tightly compartmented that he could not talk to anybody about it. Caproni told us that at some point she obtained a copy of Yoo's legal opinion. She stated that after reading it she immediately understood Philbin's concerns because the opinion appeared to lack analysis and simply concluded that the program was legal. ~~(TS//SI//NF)~~

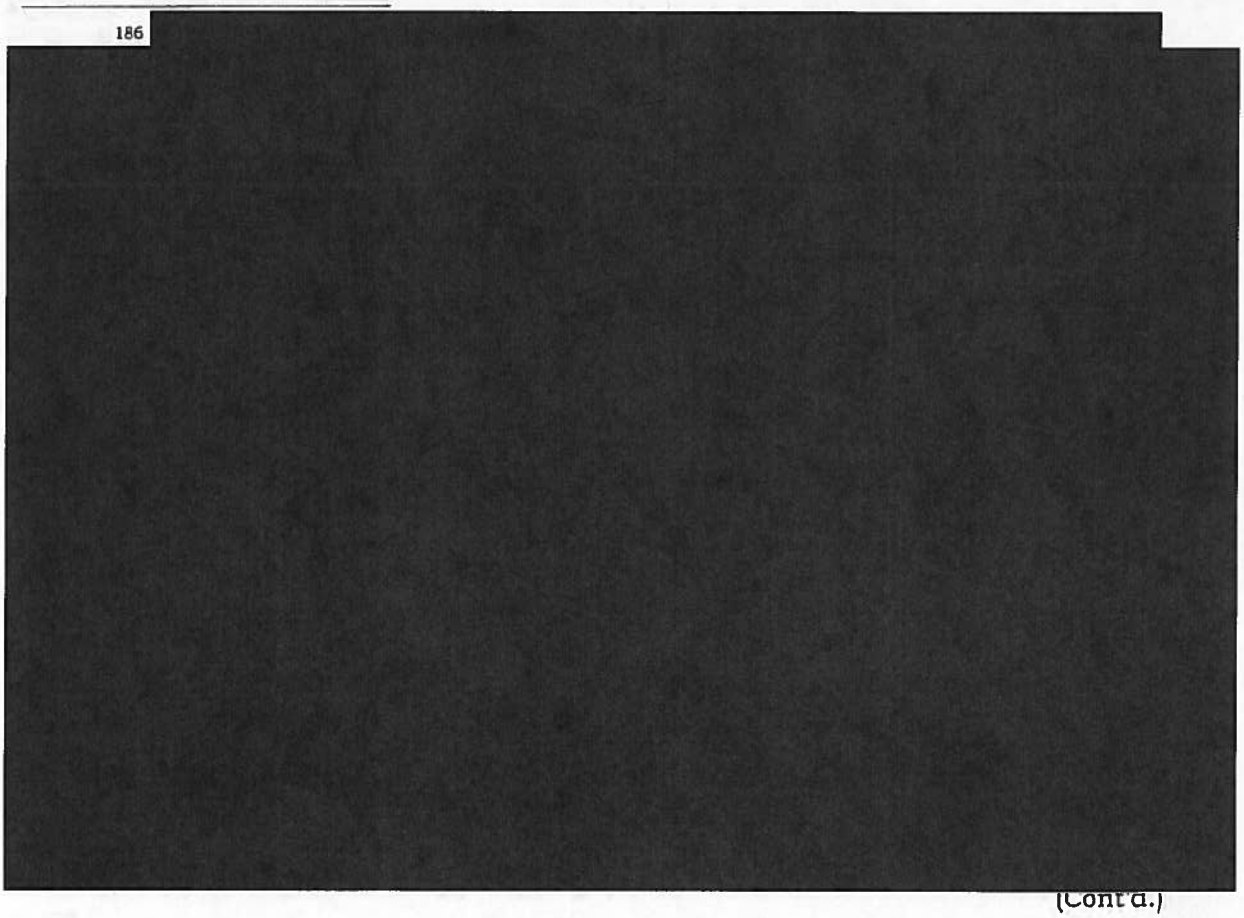
[184] The FBI's Electronic Communications Analysis Unit compiled a summary of known [redacted] Stellar Wind tip results from January 1, 2003, through mid-December 2003. However, the data included in the summary was incomplete, and the summary did not contain any analysis of the effectiveness of these tips. Another study of the [redacted] tippers was conducted in 2006. The results of that study are discussed in Chapter Six of this report, along with the OIG's analysis of the effectiveness of the program. ~~(TS//STLW//SI//OC/NF)~~



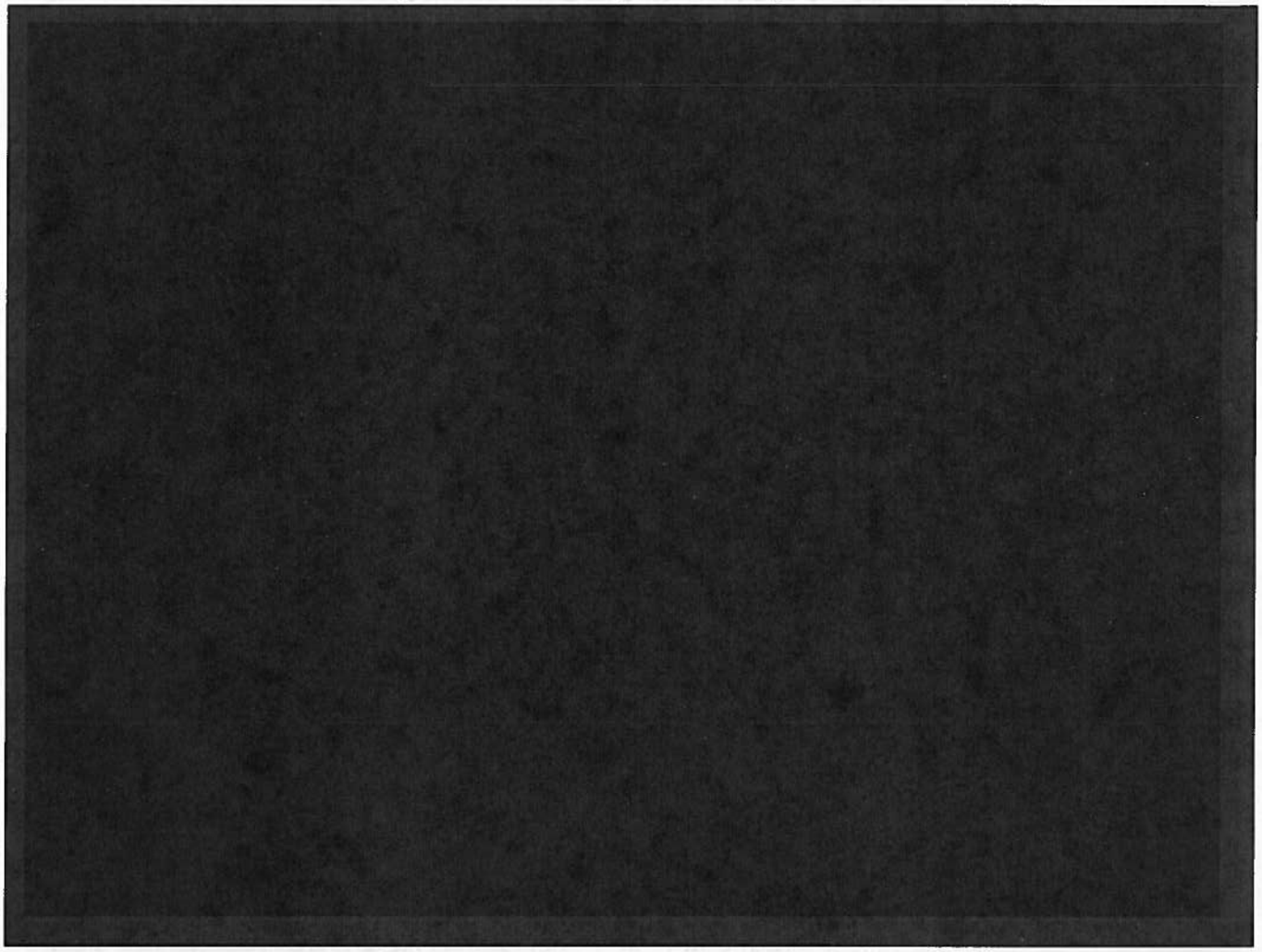
[185] Goldsmith also noted that as of the March 14, 2004, meeting, the Attorney General had not yet reported to Congress on the program under 28 U.S.C. § 530D. However, as discussed above, the White House had briefed the congressional leadership about the program on March 10, 2004. In addition, the former Presiding Judge of the FISA Court, Royce Lamberth, and the current Presiding Judge, Colleen Kollar-Kotelly, had been read into the program by this time. (U)

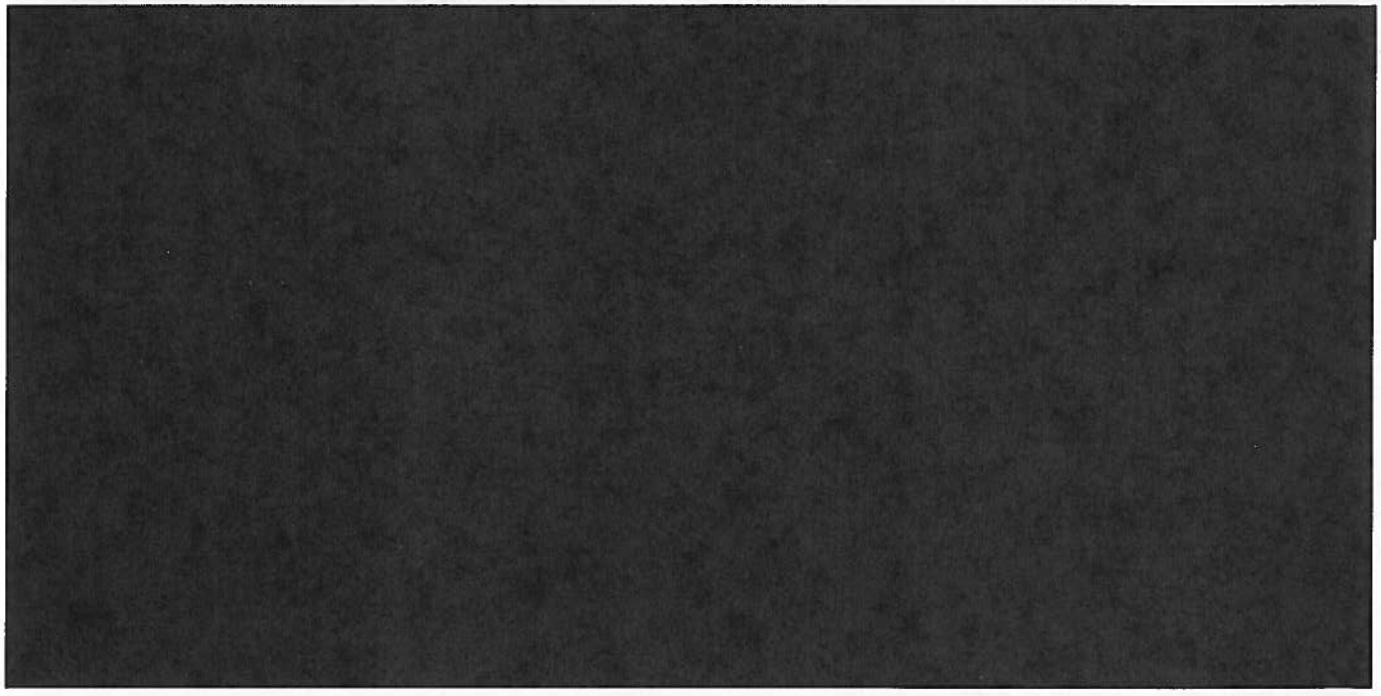


186



(Cont'd.)





[redacted]

Goldsmith told us that during his presentation of the legal analysis at the March 14 meeting he received "tough but fair and appropriate" questions from Mueller and Olson with respect to why the [redacted] ~~(TS//STLW//SI//OC/NF)~~

Goldsmith told us that the March 14 meeting was designed to achieve full consensus among the principals on the issues, and that the meeting was successful in this regard. (U)

That evening, Mueller called Gonzales to report that progress had been made, although legal support for [redacted] still had not been found. Mueller also told Gonzales that in the future Gonzales should speak directly with Comey on these matters. ~~(TS//STLW//SI//OC/NF)~~

6. Comey Determines that Ashcroft Remains "Absent or Disabled" (U)

Attorney General Ashcroft was released from the hospital at noon on March 14, 2004. The next day, Comey advised Ayres by memorandum that Ashcroft's doctor believed that Ashcroft required additional time to recuperate at home and was not yet ready to resume his responsibilities as Attorney General. Comey's memorandum noted that the doctor intended to reassess Ashcroft's condition on March 24, 2004. Comey's memorandum stated that, based on these circumstances, Comey continued to believe that Ashcroft was "absent or disabled" within the meaning of 28 U.S.C. § 508(a). Comey's memorandum concluded:

> As before, notwithstanding my continued temporary capacity as Acting Attorney General, I intend, where possible, to exercise "all the power and authority of the Attorney General" pursuant to the authority that 28 C.F.R. § 0.15(a) delegates to me in my regular capacity as Deputy Attorney General. (U)

A copy of the memorandum was sent to Gonzales at the White House and to senior Department officials.[189] (U)

7. Judge Kollar-Kotelly Briefed on Lack of Attorney General Certification (U)

As discussed earlier in this report, the extent to which OIPR could use Stellar Wind-derived information in FISA applications had been limited by Judge Kollar-Kotelly, the FISA Court's Presiding Judge. After her read-in to the program in May 2002, Judge Kollar-Kotelly had directed OIPR to continue, with some modifications, the "scrubbing" procedures for FISA applications in place at that time. ~~(TS//STLW//SI//OC/NF)~~

According to an OLC memorandum, on March 14, 2004, Judge Kollar-Kotelly was informed that the President had reauthorized the Stellar Wind program, but that the latest Authorization lacked the Attorney General's certification as to form and legality.[190] The memorandum indicated that as a result of Judge Kollar-Kotelly's uncertainty about the implications of this development, she intended to insist on a complete separation of any information derived from Stellar Wind, whether directly or indirectly, from all FISA applications presented to the FISA Court. The memorandum noted that "[b]ecause of the way tips get worked into (and lost in) the mix of intelligence information, that standard would have virtually crippled all counter-terrorism FISAs." ~~(TS//STLW//SI//OC/NF)~~

8. Comey and Gonzales Exchange Documents Asserting Conflicting Positions (U)

According to Mueller's program log, on the morning of Monday, March 15, 2004, following the daily threat briefing in the White House Situation Room, President Bush remarked to Mueller that he understood "progress had been made," referring to the discussions on the legal basis for the Stellar Wind program. Mueller called Comey shortly thereafter to convey the President's remark. Mueller suggested to Comey that additional briefings on the program should be given to Congress, including to both the House and Senate Judiciary Committees. ~~(TS//SI//NF)~~

Also on March 15, Goldsmith drafted for Comey a 3-page memorandum summarizing OLC's views with respect to the legality of the program. The memorandum recast in narrative form Goldsmith's outline of

---

[189] As discussed below, Ashcroft's doctors later cleared Ashcroft to resume his duties as Attorney General as of March 31. (U)

[190] The memorandum was prepared in anticipation of a briefing for the Attorney General on March 30, 2004. (U)

March 14, 2004 (discussed above), and noted that OLC had not reached any "final conclusions and [was] not yet prepared to issue a final opinion on the program." The memorandum also stated that the Stellar Wind program potentially implicated various congressional and intra-Executive Branch reporting requirements imposed both by statute and Executive Order. The memorandum stated that OLC was only beginning to analyze these reporting issues. ~~(TS//SI//NF)~~

Goldsmith and Philbin went to see Gonzales on the afternoon of March 15 to explain what OLC had determined in its legal analysis to that point, and also to notify Gonzales that he would be hearing from Comey shortly about the Department's position as to the program's legality. (U)

According to Philbin's contemporaneous notes on the events of the next two days, on March 16, 2004, following the morning threat briefing at the White House, Comey told President Bush that OLC had finished its preliminary legal analysis of the program.[191] Comey asked the President if Comey should convey the details of the analysis to Gonzales, and the President indicated that Comey should do so. ~~(TS//SI//NF)~~

After Comey returned to the Department, he signed a short memorandum to Gonzales that he had drafted the night before. In the memorandum, Comey first recounted how the President on March 12, 2004, had directed the Justice Department to continue its analysis of the Stellar Wind program and to "provide its best advice concerning ways to change the program to conform with the Justice Department's understanding of the applicable law." Comey then described the composition of the working group convened to accomplish this objective and how the group's efforts had resulted in Goldsmith's 3-page analysis, which Comey attached to his memorandum. ~~(TS//SI//NF)~~

Comey then set out his advice to the President. According to the memorandum, Comey advised that the President may lawfully continue [redacted] Comey wrote that [redacted] involved "close legal questions, requiring legally aggressive – indeed, novel – supporting arguments . . . ." Comey further wrote that the Department remained unable to find a legal basis to support [redacted] Accordingly, Comey advised that such [redacted]

[191] Philbin told the OIG he kept notes of these events because Comey had asked him to "keep a record." (U)

[redacted] Finally, Comey cautioned that he believed the ongoing collection of [redacted] raised "serious issues" about congressional notification, "particularly where the legal basis for the program is the President's decision to assert his authority to override an otherwise applicable Act of Congress." Comey wrote that the Department would continue to explore the notification issue. ~~(TS//STLW//SI//OC/NF)~~

Comey instructed Goldsmith and Philbin to hand deliver the memoranda to Gonzales at the White House, which they did. Philbin also delivered copies to Solicitor General Olson. Philbin's notes indicate that Olson was "annoyed" that Comey had sent the memoranda to the White House without consulting him, and asked Philbin several times, "What's my role supposed to be here?" Olson also said to Philbin that he thought the memoranda were a "poke in the eye" to the White House. Philbin wrote that Olson's reaction "raised concerns that [Comey] may have gotten himself too far out there alone" by not bringing Olson in on the Department's legal opinion in advance. (U)

Comey told us that he knew his memorandum would anger people at the White House because he had put in writing the arguments questioning the legality of aspects of the program and that the memorandum and Goldsmith's attachment would become a part of the Presidential records and would be discovered later by historians. He stated he believed it was important to "make a record." (U)

According to Mueller's program log, Gonzales called Mueller at 1:45 p.m. on March 16 to discuss the situation. Gonzales explained to Mueller that, in view of the Department's tentative conclusion that legal support for [redacted] was still lacking, Gonzales would have to make a recommendation to the President on how to proceed. Gonzales told Mueller he needed to know whether Mueller would resign if the President decided [redacted] Mueller responded that he would have to take time to consider his actions, but that he "would have to give it serious consideration if the President decided to go ahead in the face of DOJ's finding." ~~(TS//STLW//SI//OC/NF)~~

Later that afternoon on March 16, Card called Comey to the White House for a meeting. According to Philbin's notes, "the back channel word from Judge Gonzales" was that President Bush might be willing to [redacted] Prior to the meeting, Comey, Goldsmith, and Philbin agreed that Comey should be ready to convey to the White House that the Department would support [redacted] ~~(TS//STLW//SI//OC/NF)~~

Philbin's notes indicate that at the meeting Card told Comey that the President was "wrestling" with the issue of whether to [redacted] and would decide "very soon." Card also expressed to Comey his displeasure that Comey had put in writing the Department's position on the legality of the program. ~~(TS//STLW//SI//OC/NF)~~

That evening, while attending a farewell dinner for a Department colleague at a local restaurant, Philbin received a call from David Addington indicating that he wanted to deliver a letter Gonzales had written to Comey. Philbin met Addington at the Department at 8:30 p.m. that night to accept the letter. Philbin's notes also indicate that Gonzales had called Comey in advance to tell Comey "not to get too overheated by the letter." (U)

Comey told us he recalled that Gonzales told him in the call that the White House would agree to work with the Department to fix the program and that Comey should not "overreact" to Gonzales's letter. Comey said he believed Addington, and not Gonzales, had actually drafted the letter, and that Gonzales sent it only to counter Comey's memorandum and to make a record on behalf of the White House. (U)

Gonzales's letter stated that the President had directed him to respond to Comey's memorandum. The letter stated:

> Your memorandum appears to have been based on a misunderstanding of the President's expectations regarding the conduct of the Department of Justice. While the President was, and remains, interested in any thoughts the Department of Justice may have on alternative ways to achieve effectively the goals of the activities authorized by the Presidential Authorization of March 11, 2004, the President has addressed definitively for the Executive Branch in the Presidential Authorization the interpretation of the law.[192]

The letter also excerpted the language of paragraph 10 from the March 11, 2004, Authorization, which recited the bases on which the President acted to reauthorize the program, and then concluded: "Please ensure that the

[192] Gonzales's letter also addressed Comey's comments about congressional notification. Citing *Department of the Navy v. Egan*, 484 U.S. 518 (1988) and a 2003 OLC opinion, Gonzales's letter stated that the President has the constitutional authority to define and control access to the nation's secrets, "including authority to determine the extent to which disclosure may be made outside the Executive Branch." ~~(TS//STLW//SI//OC/NF)~~

Department of Justice complies with the direction given in the Presidential Authorization."[193] ~~(TS//STLW//SI//OC/NF)~~

C. White House Agrees to [redacted]

~~(TS//STLW//SI//OC/NF)~~

Notwithstanding Gonzales's letter, on March 17, 2004, the President decided to [redacted] effective at midnight on March 26, 2004. According to Mueller's program log, Gonzales called Comey to advise him of the President's decision on March 17, 2004, and Comey passed this information to Mueller later that day. Comey, in an e-mail dated March 17, expressed relief at the President's decision, writing:

> Today, in a remarkable development, we stepped back from the brink of disaster. All seems well in the Government. The right thing was done. ~~(TS//STLW//SI//OC/NF)~~

Gonzales told the OIG during his interview that he could not say whether the prospect of resignations at the Department and the FBI may have had an impact on the President's decision.[194] We were not able to interview others at the White House to determine what specifically caused the program to be modified in accord with the Department's legal position. (U)

The President's directive was expressed in two modifications to the March 11, 2004, Presidential Authorization. These modifications, as well as the operational and legal implications of the President's decision for the Department and the FBI, are described in the next sections. ~~(TS//SI//NF)~~

1. March 19, 2004, Modification (U)

On March 19, 2004, the President signed, and Gonzales certified as to form and legality, a Modification of the March 11, 2004, Presidential

---

[193] Comey stated that he did not believe Gonzales wrote this letter. He stated that "Addington was the flame-thrower" and that Gonzales was generally more reasonable and moderate. Comey said that Gonzales had later apologized to both Comey and Ashcroft for his conduct during the March 10 incident at the hospital and had even come around to agree with Philbin and Goldsmith's analysis regarding the program. Gonzales told the OIG that he did not apologize to Ashcroft for the incident in the hospital because he had been instructed by the President to go there, but stated that he "regretted" the incident. (U)

[194] However, when Gonzales commented on a draft of this report, he told the OIG that the prospect of resignations at the Department and the FBI were not the reason for the President's decision. Gonzales stated that he could not elaborate on this statement due to executive privilege considerations. (U)

Authorization. The first paragraph of the Modification stated that [redacted] The March 19 Modification made two significant changes to the existing Authorization and a third important change affecting all Authorizations. [redacted] these changes were to become effective beginning at midnight on [redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

Modification, March 19, 2004, para. 2(a)(italics and brackets added). This additional language resulted in [redacted] ~~(TS//STLW//SI//OC/NF)~~

Second, the Modification [redacted] The language, with the deleted language in brackets and the insertion indicated in italics, was:

[redacted]

[redacted]

Modification, March 19, 2004 [redacted]

Third, the March 19 Modification [redacted]

Modification, March 19, 2004 [redacted]

Each Presidential Authorization had contained a directive to the Secretary of Defense not to disclose the program outside the Executive Branch without the President's approval. The Modification reiterated that any change was not intended to reverse the President's control over access to the program. ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[195] The ultimate disposition of this previously obtained [redacted] was subsequently addressed in an April 2, 2004, Modification, and thereafter in an August 2004 Presidential memorandum to the Secretary of Defense, as described below in subsection 6. ~~(TS//STLW//SI//OC/NF)~~

[redacted][196] The President's decision to [redacted]

[redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[196] Bradbury was nominated to be Assistant Attorney General for OLC in June 2005. He was not confirmed for this position, and told us that after exhausting the time period for use of the "Acting" title under the Vacancies Reform Act of 1998 (see 5 U.S.C. § 3345 et seq.) in April 2007, he reverted to Principal Deputy Assistant Attorney General, the position he had held prior to his nomination. As head of OLC, Bradbury became responsible for briefing members of Congress on OLC's legal analyses concerning the program as well as on the Presidential Authorizations. Bradbury's access to these documents and the officials responsible for drafting them provided him significant background information on the changes to the program. (U)

[197] [redacted]

[redacted]

[redacted]

2. [redacted]

[redacted]

3. [redacted]

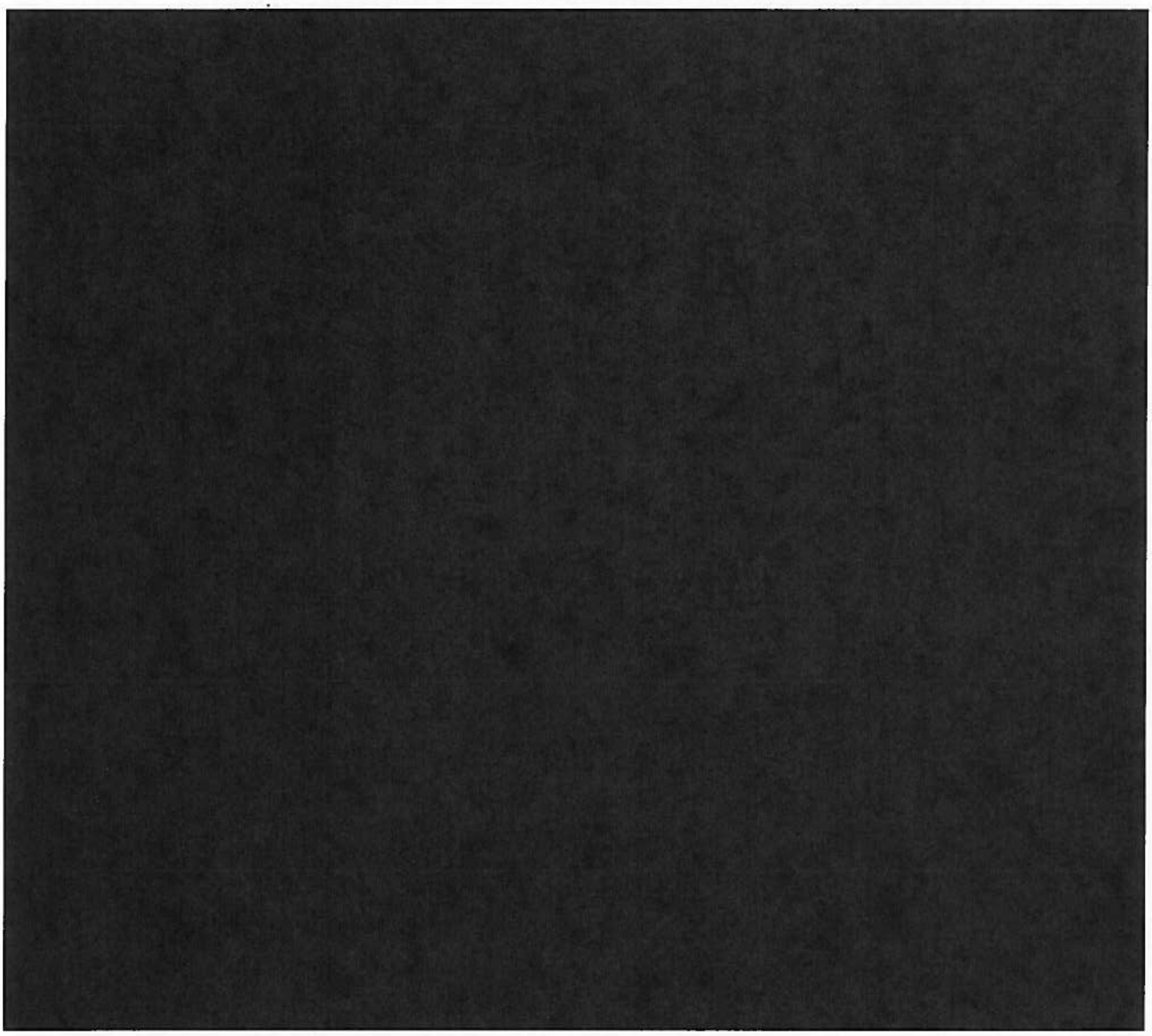
[redacted]

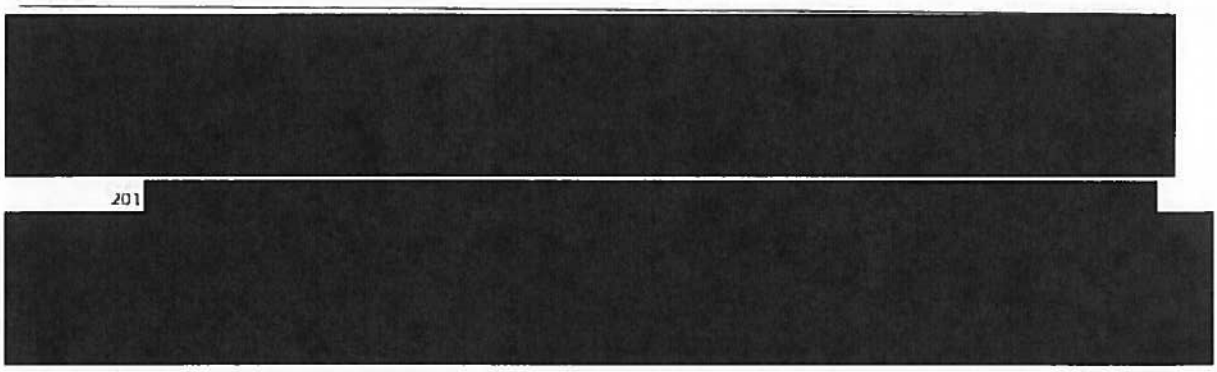
198 [redacted]

199 [redacted]

200 [redacted]

(Cont'd.)




201

4. [redacted]

5. Judge Kollar-Kotelly is Presented with the OLC Legal Analysis Regarding [redacted] ~~(TS//STLW//SI//OC/NF)~~

As noted above, Judge Kollar-Kotelly was made aware on March 14, 2004, that the March 11 Authorization had been signed by the President

but had not been certified as to form and legality by the Justice Department. On March 18, 2004, Goldsmith, Philbin, Baker, and Gonzales met with Judge Kollar-Kotelly to further brief her on the status of the program. According to an internal OLC memorandum, they advised her that forthcoming legal opinions from OLC would allay her concerns about the use of program-derived information in FISA applications.[202] ~~(TS//STLW//SI//OC/NF)~~

The OIG reviewed a handwritten letter from Judge Kollar-Kotelly to OIPR Counsel Baker, which appeared to have been written just after the initiation of [redacted] mandated in the March 19, 2004, Modification. Baker told us that the handwritten letter should be viewed as an informal draft designed to convey Judge Kollar-Kotelly's preliminary understanding of the issues raised by the changes to the Stellar Wind program. In the letter, Judge Kollar-Kotelly reiterated her position that Stellar Wind-derived information should be excluded from FISA applications, writing, "so there is no misunderstanding, I will not sign a FISA application which contains any information derived from and/or obtained from the [Stellar Wind] program," including applications in which a Stellar Wind tip "was the sole or principal factor in starting an investigation by any of the agencies, even if the investigation was conducted independently of the tip from [Stellar Wind]." Judge Kollar-Kotelly also requested, as a precondition to her agreeing to sign FISA applications in the future, that OIPR clarify in writing its proposal for reviewing FISA applications to ensure that all Stellar Wind-derived information had been excluded. Baker told us that he had a lot of "verbal back and forth" with Judge Kollar-Kotelly to explain OIPR's scrubbing procedures. ~~(TS//STLW//SI//OC/NF)~~

In late March 2004, OLC provided Judge Kollar-Kotelly with a draft analysis discussing [redacted]

---

[202] As described below, these legal opinions, which addressed the legality of [redacted] were provided to Judge Kollar-Kotelly in late March and early April 2004. ~~(TS//STLW//SI//OC/NF)~~

[203] Chapter Three, Section II B contains a description of this process. (U)

[redacted]

On March 26, 2004, OLC completed a draft memorandum for Baker entitled "Use or Disclosure of Certain Stellar Wind Information in Applications Under FISA." This memorandum addressed the inclusion in FISA applications of information derived indirectly from [redacted].[205] OLC also provided Judge Kollar-Kotelly with a copy of its draft legal analysis.[206] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

---

[204] This argument is discussed below in connection with Goldsmith's May 6, 2004, legal analysis. (U)

[205] With respect to [redacted] the memorandum stated that the Department did not believe the acquisition of such information was subject to any constitutional restraints or statutory restrictions, but that "[t]o the extent Judge Kollar-Kotelly has concerns about those conclusions, we note that the analysis in this memorandum independently demonstrates that there are no legal restrictions on the use of information indirectly derived from [redacted] tippers in FISA applications." ~~(TS//STLW//SI//OC/NF)~~

[206] The draft memorandum did not address inclusion in FISA applications of information derived *directly* from the program because OIPR had successfully managed to address Judge Kollar-Kotelly's order to exclude such information. ~~(TS//STLW//SI//OC/NF)~~

6. [redacted] Modification (U)

Attorney General Ashcroft's doctors cleared him to resume his duties as Attorney General as of March 31. Comey advised Ayres in a March 30, 2004, memorandum that as of 7:00 a.m. on March 31, the Attorney General was no longer "absent or disabled" within the meaning of 28 U.S.C. § 508(a), and that as of that time Comey could no longer exercise the duties of the Office of Attorney General pursuant to the statute. A copy of the memorandum was sent to White House Counsel Gonzales and other senior Department officials. (U)

On [redacted] President Bush signed, and Gonzales certified as to form and legality, a second Modification of the March 11, 2004, Presidential Authorization. This modification addressed only [redacted] activities of the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

[redacted]

Thus, under this new standard [redacted]

~~(TS//STLW//SI//OC/NF)~~

[redacted]

[redacted]

---

207 An April 5, 2004, Goldsmith memorandum to file stated that OLC worked with Addington to craft the new [redacted] standard. ~~(TS//STLW//SI//OC/NF)~~

208 Bradbury distinguished the limitation on [redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted] ~~(TS//STLW//SI//OC/NF)~~

7. [redacted] Standard is Conveyed to the FBI ~~(TS//SI//NF)~~

The OIG sought to determine how the presidentially authorized limitations on [redacted] in the Modifications and subsequent Authorizations were communicated to FBI employees responsible for tipping Stellar Wind information to the field. ~~(TS//STLW//SI//OC/NF)~~

A former Unit Chief in the Communications Analysis Unit (CAU) within the FBI's Communications Exploitation Section (CXS) of the Counterterrorism Division told us he became aware that at some point the scope of collection under Stellar Wind was narrowed to include only [redacted] He said this information was passed along to him and others at the FBI during either a monthly or quarterly meeting with NSA representatives. He said the [redacted] practice was "taken very seriously" by the NSA. As an example, he said that Requests for Information (RFI) from the FBI to the NSA on numbers not associated with [redacted] were rejected by the NSA as outside the scope of the revised Authorization. ~~(TS//STLW//SI//OC/NF)~~

An FBI Supervisory Special Agent in the CAU's unit co-located at the NSA (called Team 10), told us that when he first began collection and analysis work under the program, [redacted] were "fair game." He recalled that at some later point the scope of collection [redacted] He said that [redacted] was rigorously adhered to and was "scrutinized very closely." He said that when the FBI requested that the NSA collect information on a particular number, the NSA closely analyzed the number and requested supporting information from the FBI before querying the Stellar Wind database. This supervisor also stated that the NSA did a good job of keeping the co-located FBI personnel informed of changes to the scope of collections. He said this information typically would be conveyed to appropriate personnel during the daily "all hands meetings." ~~(TS//STLW//SI//OC/NF)~~

8. Office of Legal Counsel Assesses NSA's Compliance with New Collection Standards ~~(TS//SI//NF)~~

Goldsmith told us that during the week of March 29, 2004, he and Philbin conducted an "audit" of the Stellar Wind program to ensure that the querying of [redacted] was being conducted in accordance with the Presidential Authorizations. ~~(TS//STLW//SI//OC/NF)~~

Goldsmith said that while resources were not available to conduct a "professional" audit, he visited the NSA and reviewed with relevant NSA officials the legal parameters for querying [redacted] which as discussed above required a showing of reasonable articulable suspicion that the target belonged to a group that was engaged in international terrorism.[209] Goldsmith told the OIG that as part of the review, he and Philbin familiarized the NSA with the new collection parameters [redacted] ~~(TS//STLW//SI//OC/NF)~~

To conduct their review, Goldsmith and Philbin requested that the NSA [redacted] ~~(TS//STLW//SI//OC/NF)~~

On April 15, 2004, Goldsmith reported the results of his and Philbin's review to [redacted] the Assistant General Counsel for Operations in the NSA's Office of General Counsel. On April 22, 2004, Goldsmith memorialized his conversation with [redacted] in a memorandum to file. In the memorandum, Goldsmith noted four types of problems he and Philbin found in their review. [redacted] The memorandum stated that Goldsmith also conveyed this advice to Vito Potenza, the NSA's Acting General Counsel at the time. ~~(TS//STLW//SI//OC/NF)~~

9. May 5, 2004, Presidential Authorization ~~(TS//SI//NF)~~

As noted above, the March 11, 2004, Presidential Authorization, as modified, was set to expire on May 6, 2004. On May 5, the President signed another Authorization extending the Stellar Wind program through June 24, 2004. Unlike the March 11 Authorization and the two modifications that

[209] [redacted]

followed it, the May 5 Authorization was certified as to form and legality by Attorney General Ashcroft. ~~(TS//SI//NF)~~

The May 5, Authorization contained the language from the March 11 Authorization narrowing the scope of [redacted] The May 5 Authorization also included the paragraph defining the scope of [redacted] as modified on March 19 to encompass only [redacted] As to [redacted] the May 5 Authorization reiterated the new collection standard set forth in the April 2, 2004, Modification, which required that [redacted] ~~(TS//STLW//SI//OC/NF)~~

With minor variations, the collection standards and other language set forth in the May 5, 2004, Presidential Authorization remained unchanged in all of the subsequent Authorizations.[211] ~~(TS//STLW//SI//OC/NF)~~

10. May 6, 2004, OLC Memorandum ~~(TS//SI//NF)~~

On May 6, 2004, Goldsmith completed a revised OLC memorandum on the legality of the Stellar Wind program. The 108-page document stated that it was written for the Attorney General in response to his request for OLC "to undertake a thorough reexamination of the Stellar Wind program as it is currently operated to confirm that the actions that the President has directed the Department of Defense to undertake through the National Security Agency (NSA) are lawful." ~~(TS//SI//NF)~~

The memorandum traced the history of the program and analyzed the legality of each of the three collection baskets in light of applicable statutes, Executive Orders, cases, and constitutional provisions. ~~(TS//STLW//SI//OC/NF)~~

---

210 This Authorization also dropped the language describing [redacted] in the March 11, 2004, Authorization. ~~(TS//SI//NF)~~

211 [redacted]

The memorandum noted that Section 111 of FISA, 50 U.S.C. § 1811, providing that the President "may authorize electronic surveillance without a court order . . . to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by Congress," made it clear that FISA expressly addresses electronic surveillance during wartime.[212] The memorandum stated that the Authorization for Use of Military Force (AUMF) passed by Congress shortly after the attacks of September 11, 2001, gave the President authority to use both domestically and abroad "all necessary and appropriate force," including signals intelligence capabilities, to prevent future acts of international terrorism against the United States. According to the memorandum, the AUMF was properly read as an express authorization to conduct targeted electronic surveillance against al Qaeda and its affiliates, the entities responsible for attacking the United States. ~~(TS//STLW//SI//OC/NF)~~

The memorandum noted that the legislative history of FISA indicates that the 15-day window was "thought sufficient for the President to secure legislation easing the restrictions of FISA for the conflict at hand." Quoting H.R. Conf. Rep. No. 95-1720, at 34, reprinted in U.S.C.C.A.N. 4048, 4063 ("[T]he conferees intend that this period will allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency"). According to the OLC memorandum, "The Congressional Authorization functions as precisely such legislation: it is emergency legislation passed to address a specific armed conflict and expressly designed to authorize whatever military actions the Executive deems appropriate to safeguard the United States." ~~(TS//SI//NF)~~

The memorandum concluded that at a minimum the AUMF made the application of FISA in a wartime context sufficiently ambiguous that the doctrine of constitutional avoidance properly applied to avoid a conflict between FISA and the presidentially authorized Stellar Wind program. Alternatively, the memorandum argued that FISA, as applied in the particular circumstances of a President directing surveillance of the enemy to prevent future attacks upon the nation, represented an unconstitutional infringement on the President's Article II Commander-in-Chief powers. ~~(TS//STLW//SI//OC/NF)~~

These two arguments also were cited in support of [redacted]

[212] As discussed in section I of this chapter, the legal implications of this provision of FISA was not addressed in the memoranda John Yoo had drafted in support of the program in late 2001. ~~(TS//SI//NF)~~

[redacted]

The memorandum also analyzed the legal rationale for [redacted]

[redacted] (~~TS//STLW//SI//OC/NF~~)

[redacted]

[redacted]

[redacted]

[redacted]

213 [redacted]

[redacted]

Finally, the memorandum discussed the Fourth Amendment implications of the Stellar Wind program. To determine whether interception of [redacted] violated the Fourth Amendment's prohibition against unreasonable searches, the memorandum analyzed whether the importance of the government's interest in this collection outweighed the individual privacy interests at stake. Citing various authorities, including Supreme Court opinions, the Federalist Papers, [redacted] and congressional testimony, the memorandum concluded that "the government's overwhelming interest in detecting and thwarting further al Qaeda attacks is easily sufficient to make reasonable the intrusion into privacy involved in intercepting selected communications." The memorandum noted that the weight of the

214 [redacted]

215 [redacted]

government's interest in this regard could change over time if the threat from al Qaeda were deemed to recede. ~~(TS//STLW//SI//OC/NF)~~

The memorandum also analyzed telephone and e-mail meta data collection under the Fourth Amendment. The memorandum concluded, based on the Supreme Court's holding in *Smith v. Maryland*, 442 U.S. 735, 742 (1979), that there is no legitimate expectation of privacy in the numbers dialed to place telephone calls. Referring to cases holding that no expectation of privacy attached to the address information on either letter mail or e-mail, the memorandum concluded that no Fourth Amendment privacy interests were implicated in the collection of e-mail meta data. ~~(TS//STLW//SI//OC/NF)~~

In sum, the May 6 memorandum was the most comprehensive assessment of the Stellar Wind program drafted by the Office of Legal Counsel. [redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted] ~~(TS//STLW//SI//OC/NF)~~
~~(TS//STLW//SI//OC/NF)~~

III. OIG Analysis (U)

A. Department's Access to and Legal Review of Stellar Wind Program Through May 2004 ~~(TS//SI//NF)~~

The Justice Department's access to the Stellar Wind program was controlled by the White House, and Gonzales told the OIG that the President decided whether non-operational personnel, including Department lawyers, could be read into the program. Department and FBI officials told us that obtaining approval to read in Department officials and FISA Court judges involved justifying the requests to Addington and Gonzales, who effectively acted as gatekeepers to the read-in process for non-operational officials. In contrast, according to the NSA, operational personnel at the NSA, CIA, and the FBI were read into the program on the authority of the NSA Director, who at some point delegated this authority to the Stellar Wind Program Manager. ~~(TS//SI//NF)~~

Various officials we interviewed about the issue uniformly agreed that the White House sought to strictly limit overall access to the Stellar Wind program. We believe that this policy was applied at the Department in an unnecessarily restrictive manner prior to March 2004, and was detrimental to the Department's role in the operation of the program through that period. We also believe that Attorney General Ashcroft, as head of the Department, was responsible for seeking to ensure that the Department had adequate attorney resources to conduct a thorough and accurate review of the legality of the program. Because Ashcroft did not agree to be interviewed for this investigation, we were unable to determine the extent of his efforts to press the White House to read in additional Department officials between the program's inception in October 2001 and the critical events of March 2004. ~~(TS//SI//NF)~~

In Chapter Three we described how the Department's early involvement in the Stellar Wind program was limited to the participation of only three attorneys – Attorney General Ashcroft, OLC Deputy Assistant Attorney General John Yoo, and Counsel for Intelligence Policy James Baker.[216] Working alone, Yoo drafted several legal memoranda in 2001 and 2002 advising the Attorney General and the White House that the program was legally supported. In reliance on Yoo's advice, Attorney General Ashcroft certified the legality of the Presidential Authorizations to implement the program. ~~(TS//SI//NF)~~

Because Yoo worked alone, his legal analysis was not reviewed by other attorneys, either in OLC or elsewhere in the Department.[217] Even

---

[216] Counsel for Intelligence Policy James Baker was read into the program in either late 2001 or January 2002. But Baker appears to have been read in only because he inadvertently came across information that suggested such a program existed. While Baker had involvement in several aspects of the program, he had no involvement in drafting or reviewing Yoo's legal memoranda supporting the program. Daniel Levin, who served as both Chief of Staff to FBI Director Mueller and briefly as a national security counselor to Ashcroft, also was read into Stellar Wind at the inception of the program. However, Levin only served for two months at the Department during this early phase of Stellar Wind and had very limited involvement in the program during this period. Levin told us he was read into Stellar Wind along with Director Mueller at the FBI and that he understood that he was being cleared into the program as an FBI official. We therefore consider Levin to be an FBI read-in, not a Department read-in. ~~(TS//STLW//SI//OC/NF)~~

[217] Gonzales told us that he thought Yoo may have assigned discrete tasks to other attorneys in connection with his work on the Stellar Wind legal memoranda. Because Yoo declined our request for an interview, we were unable to confirm this. In any event, no other attorneys were read into Stellar Wind and therefore would not have been permitted to work on or review those portions of the memoranda that contained Top Secret/Sensitive Compartmented Information (TS/SCI) related to the Stellar Wind program. By contrast, Yoo had at least one other OLC attorney to assist him in drafting other OLC legal memoranda on the detainee interrogation program during the 2001 to 2003 period, and these memoranda were reviewed by another OLC Deputy Assistant Attorney General

(Cont'd.)

when Jay Bybee became the OLC Assistant Attorney General in November 2001, and was therefore Yoo's supervisor, Bybee was not read into the program.[218] Bybee told us he also was unaware that Yoo was providing advice to the Attorney General and the White House on the legal basis to support the program. ~~(TS//SI//NF)~~

We believe that even before Patrick Philbin voiced his initial concerns with Yoo's analysis in 2003, the circumstances in 2001 and 2002 plainly called for additional Department resources to be applied to the legal review of the program and that it was the Attorney General's responsibility to be aware of this need and to take steps to address it. Moreover, because Ashcroft met frequently with the President on national security matters, he would have been well-positioned to request additional legal resources if he believed they were necessary. ~~(TS//SI//NF)~~

The facts suggest that Ashcroft had some awareness and concern that Yoo was working on the legal justification for the Stellar Wind program without any Department assistance or oversight, and possibly was advising the White House directly of his findings. Based on accounts of the incident in Ashcroft's hospital room in March 2004, Ashcroft made specific complaints to Gonzales and Card about insufficient legal resources at the Department and that the Department had been "cut out of the whole affair." He had also expressed frustration to Comey months earlier about being "in a box" with Yoo. Further, according to Goldsmith, when Goldsmith first interviewed for the position of Assistant Attorney General for OLC in 2003, Ashcroft and his Chief of Staff alluded to concerns over being kept informed of matters the Office of Legal Counsel was working on and the importance of keeping the Attorney General "in the loop." We also note that Yoo's November 2, 2001, memorandum to Ashcroft indicated that "[b]ecause of the highly sensitive nature of this subject and the time pressures involved, this memorandum has not undergone the usual editing and review process for opinions that issue from our Office [OLC]." ~~(TS//SI//NF)~~

While we believe that Ashcroft may have been aware that Yoo was working alone on the Stellar Wind analysis and had concerns about this, we do not know whether or how hard he pressed the White House to read in additional attorneys to assist or supervise Yoo. At the same time, however,

---

(Philbin) and approved by the OLC Assistant Attorney General (Bybee). The detainee interrogation program also was classified as TS/SCI. We also note that Philbin's background in telecommunications law would have made him a logical choice to assist Yoo on the Stellar Wind legal analysis. ~~(TS//SI//NF)~~

[218] In contrast, Bybee was allowed to supervise Yoo's work drafting legal memoranda concerning a detainee interrogation program during the same time period. ~~(TS//SI//NF)~~

we cannot assume that any requests by Ashcroft for additional attorney read-ins would have been granted by the White House. Gonzales told us that Ashcroft had requested that Deputy Attorney General Larry Thompson and Ashcroft's Chief of Staff David Ayres be read in. However, neither request was approved.[219] Gonzales stated that he did not recall Ashcroft requesting additional read-ins beyond Thompson and Ayres. (U)

In analyzing the read-in situation at the Department during Yoo's tenure, we also considered that Ashcroft certified the program as to its legality each time the program came up for renewal, and did so at a time when Yoo's legal advice was the only Department guidance available concerning the program's legality. We believe the fact that only three Department attorneys were read into Stellar Wind through mid-2003 may have been due at least in part to Ashcroft's routine recertifications of the Presidential Authorizations during this period. As noted in Chapter Three, Gonzales told us that it was up to the Attorney General to decide how to satisfy his legal obligations as Attorney General, and that if Ashcroft believed more attorneys were needed for this purpose, he could have asked the President to approve additional Department read-ins. Gonzales also told us that Ashcroft's continued certifications of the Presidential Authorizations supported Gonzales's belief that Ashcroft was satisfied with the quality of the legal advice he was receiving at the time within the Department. ~~(TS//SI//NF)~~

There is evidence as well that Gonzales, as White House Counsel, was satisfied with Yoo's legal memoranda supporting the program. Gonzales told us that although he did not believe Yoo's first two memoranda fully addressed the White House's understanding of the Stellar Wind program, Gonzales believed that they described as lawful activities that were broader than those carried out under Stellar Wind, and that Yoo's memoranda therefore "covered" the program.[220] ~~(TS//SI//NF)~~

---

[219] Deputy Attorney General Thompson resigned from the Department in August 2003, so Ashcroft's request to have him read into the program would have been made before that time. That neither Thompson nor Ayres was read in contrasts with the decision to allow in the case of [redacted] to be briefed about the program in 2002, and [redacted] to be read into the program in 2003. The OIG does not know who authorized these read-ins. ~~(TS//SI//NF)~~

[220] We were troubled by Gonzales's suggestion that Yoo's memoranda covered the program because the memoranda determined to be lawful a range of "hypothetical" activities that were interpreted by Gonzales to be broader than those actually carried out under Stellar Wind. Such an approach, if deemed acceptable by the "client" (in this case the White House), would encourage the Office of Legal Counsel to draft broad and imprecise (Cont'd.)

However, even apart from the limited number of Department read-ins, we believe that the White House imposed excessively strict controls over access to the program in other ways that were detrimental to the Department's ability to provide the White House with the soundest possible legal advice. For instance, we found no indication that Yoo coordinated his legal analysis with the NSA. According to Michael Hayden, the Director of the NSA when Stellar Wind began, the NSA relied on its Office of General Counsel, and not the Department of Justice, for advice as to the legality of the program when it was created. However, we found that the NSA's Office of General Counsel did not coordinate its legal advice with the Department, and even as late as 2003 the NSA General Counsel was prevented by the White House from reviewing the Department's legal opinions on the program.[221] Hayden also told the OIG that he was "surprised with a small 's'" that the Department did not participate in the early meetings with him and White House officials when Stellar Wind was first conceived. In addition, Addington instructed Philbin not to discuss the program with Baker, who as Counsel for Intelligence Policy was responsible for representing the government before the FISA Court.[222] ~~(TS//SI//NF)~~

We believe that that White House should have allowed and even encouraged coordination between the Department and the NSA regarding the development of the legal analysis of the program, especially as this analysis was first being formulated in late 2001. Such interaction between the Department and other Executive agencies is a mainstay of traditional OLC practice, and we believe its absence here contributed to factual errors in Yoo's opinions regarding the operation of the program. ~~(TS//SI//NF)~~

Although we could not determine exactly why Yoo remained the only Department attorney assigned to assess the program's legality from 2001 until his departure in May 2003, we discuss below our belief that this practice represented an extraordinary and inappropriate departure from OLC's traditional review and oversight procedures and resulted in significant harm to the Department's role in the program. ~~(TS//SI//NF)~~

When Yoo left the Department in May 2003, he was replaced by Patrick Philbin, who was read into the program to advise Ashcroft whether he could continue to certify the Presidential Authorizations as to their form

---

legal analysis and would discourage the type of careful scholarship to which the OLC traditionally aspires. ~~(TS//SI//NF)~~

[221] In addition, the NSA Office of the Inspector General, which wanted to conduct an internal audit of the program during this period, was prevented by Addington from reviewing the Justice Department's legal memoranda supporting the program. (U//~~FOUO~~)

[222] Philbin told the OIG that he spoke with Baker about the program despite Addington's instruction not to. (U)

and legality. When Goldsmith became the OLC Assistant Attorney General in October 2003, Philbin pressed Addington to have Goldsmith read in, and Goldsmith became the first head of OLC to be read into the program. As noted, Goldsmith's predecessor Jay Bybee was never read into the program. ~~(TS//SI//NF)~~

Thus, by the end of 2003, a total of only 5 Department officials – Yoo, Ashcroft, Baker, Philbin, and Goldsmith – had been read into Stellar Wind. By comparison, and as shown in Chart 4.1 below, we determined that many other individuals throughout the government were read into the program. Through the same period, [redacted]

~~(TS//STLW//SI//OC/NF)~~

[redacted]

The assignment of only one Department attorney, John Yoo, to conduct a legal review of the program without assistance or oversight from anyone else at the Department, combined with the White House's decision to prevent the NSA from reviewing Yoo's work, resulted in legal opinions by Yoo that were later determined by OLC to be so inaccurate and incomplete

---

[223] This table was derived from NSA read-in information. Justice Department read-ins include [redacted] OIG personnel who were read into Stellar Wind in 2006. (U//~~FOUO~~)

as to be regarded as not covering key aspects of the Stellar Wind program. Given the enormously complex nature of the program from both a technical and legal perspective, coupled with the fact that he was working alone, it was not altogether surprising that Yoo's analysis contained inaccuracies and omitted critical elements, particularly given the pressure to generate a legal analysis within weeks of the program's implementation. However, Yoo's analysis did not change or include a more accurate description of the program's operation over the course of his 20-month tenure with the OLC. ~~(TS//SI//NF)~~

After reviewing Yoo's legal opinions on the program, Goldsmith and Philbin quickly discovered what they characterized as serious flaws in Yoo's legal analysis. These flaws included Yoo's failure to describe [redacted] being conducted by the NSA under the Stellar Wind program and his failure to assess the legality of this and other activities as they were carried out by the NSA. ~~(TS//STLW//SI//OC/NF)~~

Specifically, both Goldsmith and Philbin stated that Yoo mischaracterized in his memoranda the nature and scope of the NSA's [redacted] They stated that Yoo's characterization of this activity in his 2001 and 2002 legal memoranda was factually flawed and that Yoo appears to have based his legal analysis of this aspect of the program on an incomplete and inaccurate description both of [redacted] and the [redacted][224] Both Goldsmith and Philbin also acknowledged that they initially incorrectly believed the NSA's [redacted] was broader than it in fact was under the program. However, unlike Yoo, Goldsmith and Philbin accurately

[224] [redacted]

characterized the collection [redacted] and thus their legal advice was based on facts that more closely reflected the actual operation of the program.[225] ~~(TS//STLW//SI//OC/NF)~~

In addition, Goldsmith and Philbin discovered that Yoo's assertion that the President had broad authority to conduct electronic surveillance without a warrant pursuant to his Commander-in-Chief powers under Article II of the Constitution, particularly during wartime, never addressed the FISA provision that expressly addressed electronic surveillance following a formal declaration of war. See 50 U.S.C. § 1811. Goldsmith also criticized Yoo's legal memoranda for failing to support Yoo's aggressive Article II Commander-in-Chief theory with a fully developed separation of powers analysis, and instead offering only sweeping conclusions. As an example, Goldsmith cited Yoo's assertion that reading FISA to be the "exclusive statutory means for conducting electronic surveillance for foreign intelligence" amounts to an "unconstitutional infringement on the President's Article II authorities."[226] Moreover, noted Goldsmith, Yoo omitted from his separation-of-powers discussion any analysis of how the Youngstown Steel Seizure Case, a seminal Supreme Court decision on the distribution of governmental powers between the Executive and Legislative Branches during wartime, would affect the legality of the President's actions with respect to Stellar Wind.[227] ~~(TS//STLW//SI//OC/NF)~~

In reliance on Yoo's advice, the Attorney General certified the program "as to form and legality" some 20 times before Yoo's analysis was determined to be flawed by his successors in OLC and by attorneys in the Office of the Deputy Attorney General. We agree with many of the criticisms offered by Department officials regarding the practice of allowing a single Department attorney to develop the legal justification for the program

[redacted]

[225] [redacted]

[redacted]

[226] See Yoo Memorandum, November 2, 2001, at 9. Yoo went on to state that [redacted] Yoo concluded that FISA "represents a statutory procedure that creates a safe harbor for surveillance for foreign intelligence purposes." Id. ~~(TS//SI//NF)~~

[227] The Department's Office of Professional Responsibility (OPR) intends to review whether Yoo's legal analysis concerning the Stellar Wind program violated any standards of professional conduct. OPR has similarly reviewed whether the legal analysis by Yoo and others concerning the detainee interrogation program violated standards of professional conduct. ~~(TS//SI//NF)~~

during its early stage of operation. We summarize these criticisms below. ~~(TS//SI//NF)~~

Goldsmith described as "crazy" and "outrageous" the assignment of an OLC Deputy Assistant Attorney General to provide legal advice to the White House without the knowledge or concurrence of the Senate-confirmed Assistant Attorney General for OLC, who is accountable for the legal positions taken by the office. (U)

Goldsmith said that not a single critical eye reviewed Yoo's work on a program that Goldsmith described as "flying in the face" of the conventional understanding of the law at the time. Goldsmith noted that Yoo's legal memoranda did not include facts about how the Stellar Wind program operated in practice, and he surmised that Yoo instead might have "keyed off" the Presidential Authorizations rather than NSA's actual collection practices in developing his analysis. Goldsmith also said it was "insane" that Yoo's memoranda were not shared with the NSA. Goldsmith said that had the NSA reviewed these memoranda Yoo's failure to accurately describe the nature and scope of the collection by the NSA and the resulting "mismatch" between the actual practice and the wording of the Presidential Authorizations might have been detected earlier. ~~(TS//SI//NF)~~

Similarly, Daniel Levin, who was one of the first FBI officials to be read into Stellar Wind and who would later become Acting Assistant Attorney General for OLC upon Goldsmith's departure in June 2004, criticized allowing a single attorney to be the sole voice of the OLC concerning a program such as Stellar Wind. Levin stated that OLC has a special role at the Department and within the government, especially with "highly secret programs where opinions may never see the light of day." Under such circumstances, according to Levin, it is very difficult not to say "yes" to the White House – OLC's client – in the face of national security threats. Levin stated that unlike situations where a court places limitations on the positions the government may take, there are no such limitations when OLC considers a position that will remain secret, and it is easier to be more aggressive and "cut some corners" under such circumstances. ~~(TS//STLW//SI//OC/NF)~~

Levin stated that Yoo's memoranda justifying the program suffered from too little circulation and a lack of alternative views. He said that the OLC memoranda produced under Goldsmith's tenure were better, not because the authors were "smarter" than Yoo, but because the authors benefited from multiple viewpoints and input. Levin also said that he never understood why the Stellar Wind program was deemed so sensitive at the operational level. Levin said he appreciated that the program was politically sensitive, but added that it was a "huge mistake" to keep the program so closely held within the Department. ~~(TS//STLW//SI//OC/NF)~~

We believe that Goldsmith's and Levin's comments concerning the secrecy of Stellar Wind are especially relevant to the need for legally and factually sound OLC analysis with respect to classified national security programs. Because programs like Stellar Wind are not subject to the usual external checks and balances on Executive authority, OLC's advisory role is particularly critical to the Executive's understanding of potential statutory and Constitutional constraints on its actions. ~~(TS//STLW//SI//OC/NF)~~

Deputy Attorney General Comey also criticized the decision to allow a single person to assess the legality of the program on behalf of the Department. Comey told us that Goldsmith had once aptly described the Yoo situation to him as "the perfect storm" in which the following factors converged: the terrorist attacks of September 11, 2001; a "brilliant guy" at the Department who was "an aggressive advocate for executive power"; and a White House "determined to restore executive power." Comey expressed a degree of sympathy for Yoo, noting the extraordinary situation into which Yoo had been placed. Comey also observed that the response to September 11 essentially placed the policy burden on lawyers, who were now looked to by others for guidance as to what counterterrorism activities fell within the bounds of the law. However, Comey said that he believed White House officials "got what they ordered" by asking Yoo for opinions and restricting the number of persons with access to the program or the opinions.[228] ~~(TS//SI//NF)~~

Attorney General Ashcroft declined to be interviewed in our review, and we were thus unable to determine what his views were on the assignment of Yoo alone to conduct the legal review of the program. However, as noted above, witness accounts of his statements concerning the Yoo situation leave little doubt that Ashcroft was plainly upset with the White House for putting him "in a box" with Yoo. According to Goldsmith and Philbin, Ashcroft was direct about his grievances when Gonzales and Card came to see him in the hospital on March 10, 2004, including complaining that Ashcroft's Chief of Staff and until recently the Deputy Attorney General had not been allowed to be read into the program, and that he found it "very troubling that [redacted] people in other agencies" had been read into the program. What remains unclear is whether Ashcroft came to the realization that the Department had been given an insufficient number of read-ins only after Philbin and Goldsmith presented him with their concerns about the quality of Yoo's legal analysis, or at some point before. ~~(TS//SI//NF)~~

---

[228] As noted in Chapter Three, Yoo had been given the national security portfolio when he first joined the OLC in July 2001, several months before the attacks of September 11, 2001, and the inception of Stellar Wind. (U//~~FOUO~~)

We sought to obtain Yoo's and the White House's perspective on his selection as the sole Justice Department attorney to be read into Stellar Wind to provide advice on the legality of the program. We were not able to interview Yoo, who declined our request, or Addington and Card, who did not respond to our requests. ~~(TS//SI//NF)~~

The OIG asked Gonzales about how the White House determined who in the Department could be read into the program, but on the advice of Special Counsel to the President, Gonzales limited his answer to his personal views and declined to discuss internal White House deliberations that may have factored into the read-in decisions. Gonzales stated that he believed it was necessary for national security reasons to limit the number of read-ins to those "who were absolutely essential." Gonzales also stated that there had to be sufficient operational personnel at the NSA, CIA, and FBI read in for the purpose of running the program, while reading in additional lawyers at the Department had comparatively less value because all lawyers will "have opinions" about the program. Yet, Gonzales also stressed to us that he welcomed the Department's reassessment of Yoo's opinions and encouraged Goldsmith and Philbin to re-examine the legal basis for the program in 2003 and 2004.[229] ~~(TS//SI//NF)~~

We think the proposition that the participation of Department attorneys to analyze the legality of a program as factually and legally complex as Stellar Wind should be limited for the reasons offered by Gonzales is shortsighted and counterproductive. First, it is evident that Stellar Wind was as legally complex as it was technically challenging. Just as a sufficient number of operational personnel were read into the program to assure its proper technical implementation, we think as many attorneys as necessary should have been read in to assure the soundness of the program's legal foundation. This was not done during the early phase of the program. ~~(TS//SI//NF)~~

The full history of the program also indicates that the program benefited from additional attorney read-ins. In this chapter, we described how Philbin and Goldsmith – who held differing opinions on which legal theory best supported the program – discovered serious deficiencies in Yoo's analysis and together drafted more factually accurate and legally thorough support for the program. In Chapters Five, Six, and Seven we further describe how reading in additional attorneys facilitated the grounding of the program on firmer legal footing under FISA, allowed the Department more efficiently to "scrub" Stellar Wind-derived information in FISA applications,

---

[229] As discussed in this chapter, Comey, Goldsmith, and Philbin generally agreed that Gonzales supported the Department's legal reassessment of the program. They also characterized Addington as far less supportive of their work than Gonzales. ~~(TS//SI//NF)~~

and improved the handling of Stellar Wind-related discovery issues in international terrorism prosecutions. ~~(TS//STLW//SI//OC/NF)~~

Second, we do not believe that reading in a few additional Department attorneys during the first 2 years of the program would have jeopardized national security as suggested by Gonzales, especially given the hundreds of operational personnel who were cleared into the program during the same period (see Chart 4.1). In fact, as noted above, we think the highly classified nature of the program, rather than constituting an argument for limiting the OLC read-ins to a single attorney, made the need for careful analysis and review within the Department and by the NSA only more compelling. ~~(TS//SI//NF)~~

In sum, we concluded that the departure from established OLC and Department practices resulted in legal opinions to support the program that were later determined to be flawed. We believe the strict control over the Department's access to the program undermined the role of the Department to ensure the legality of Executive Branch actions, and as discussed below, contributed to the March 2004 crisis that nearly resulted in the mass resignation of the Department's leadership. ~~(TS//SI//NF)~~

We recommend that when the Justice Department is involved with such programs in the future, the Attorney General should carefully assess whether the Department has been given adequate resources to carry out its vital function as legal advisor to the President and should aggressively seek additional resources if they are found to be insufficient. We also believe that the White House should allow the Department a sufficient number of read-ins when requested, consistent with national security considerations, to ensure that sensitive programs receive a full and careful legal review. (U)

B. The Hospital Visit (U)

The Department's reassessment of Yoo's analysis led Comey, who was exercising the powers of the Attorney General while Ashcroft was hospitalized in March 2004, to conclude that he could not certify the legality of the Stellar Wind program. In response, the President sent Gonzales and Chief of Staff Andrew Card to visit Ashcroft in the hospital to seek his certification of the program, an action Ashcroft refused to take. We believe that the way the White House handled its dispute with the Department about the program – particularly in dispatching Gonzales and Card to Ashcroft's hospital room to override Comey's decision – was troubling for several reasons. ~~(TS//SI//NF)~~

As discussed in this chapter, by March 2004, when the Presidential Authorization was set to expire again, Goldsmith had placed Gonzales and Addington on notice for several months of the Department's doubts about

the legality of aspects of the Stellar Wind program. In particular, he and Philbin had made clear that the Department questioned the legality of the collections of [redacted].[230] ~~(TS//STLW//SI//OC/NF)~~

After Attorney General Ashcroft was hospitalized and unable to fulfill his duties, the White House was informed that Deputy Attorney General Comey had assumed the Attorney General's responsibilities. We found that the assertion by some in the White House at the time that they had not been informed of the situation was subsequently contradicted by the facts. In particular, Gonzales later acknowledged that he was aware that Comey was acting as the Attorney General.[231] (U)

Before the Presidential Authorization was set to expire on March 11, Comey, who was exercising the powers of the Attorney General at the time, told top officials in the White House – including Vice President Cheney and White House Counsel Gonzales – that the Justice Department could not recertify the legality of the program as it was presently operating. The White House disagreed with the Justice Department's position, and on March 10, 2004, convened a meeting of eight congressional leaders to brief them on the Justice Department's seemingly sudden reluctance to recertify the program and on the need to continue the program. The White House did not invite anyone from the Department to this briefing to describe the basis for its advice about the legality of the program, nor did it inform the Department of its intention to hold the meeting.[232] ~~(TS//SI//NF)~~

Following this briefing, Gonzales and Card went to the hospital to ask Attorney General Ashcroft, who was in the intensive care unit recovering

---

[230] Our conclusion that Goldsmith advised Gonzales and Addington of the Department's concerns in December 2003 is supported by his contemporaneous notes of these events. In addition, although Gonzales told us that the first time he recalled hearing of these concerns in detail was in early March 2004, he did not dispute that Goldsmith had first begun to advise him of the Department's general concerns months earlier. (U)

[231] During his congressional testimony, when questioned about whether he knew that Attorney General Ashcroft's powers had been transferred to Comey, Gonzales responded, "I think that there were newspaper accounts, and that fact that Mr. Comey was the acting Attorney General is probably something I knew of." (U)

[232] On the advice of White House counsel, Gonzales declined to provide a reason to the OIG why the Department was not asked to participate in the briefing. However, when Gonzales commented on a draft of this report, he stated that the purpose of the meeting was to inform the congressional leaders that the Department had a problem with the legal basis for aspects of the program, [redacted] and that a legislative fix therefore was necessary. Gonzales stated that the purpose of the meeting was not to have a "debate" between the White House and the Department concerning the legality of the program, but rather to explore just such a legislative "fix." ~~(TS//SI//NF)~~

from surgery and according to witnesses appeared heavily medicated, to certify the program, notwithstanding Comey's stated opposition. Yet, they did not notify Comey or anyone else in the Department that they intended to take this action. Their attempt to have Ashcroft recertify the program did not succeed. Ashcroft told them from his hospital bed that he supported the Department's legal position, but that in any event he was not the Attorney General at the time – Comey was. (U)

Gonzales stated that even if he knew that Ashcroft was aware of Comey's opposition to recertifying the program, Gonzales would still have wanted to speak with Ashcroft because he believed Ashcroft still retained the authority to certify the program. Gonzales testified before the Senate Judiciary Committee in July 2007 that although there was concern over Ashcroft's condition, "We would not have sought nor did we intend to get any approval from General Ashcroft if in fact he wasn't fully competent to make that decision." Gonzales also testified, "There's no governing legal principle that says that Mr. Ashcroft, if he decided he felt better, could decide, 'I'm feeling better and I can make this decision, and I'm going to make this decision.'" (U)

We found this explanation and the way the White House handled the dispute to be troubling. Rather, we agree with Director Mueller's observation, as recorded in his program log following his meeting with Card on March 11, 2004, that the failure to have Department of Justice representation at the congressional briefing and the attempt to have Ashcroft certify the Authorization by overruling Comey "gave the strong perception that the [White House] was trying to do an end run around the Acting [Attorney General] whom they knew to have serious concerns as to the legality of portions of the program." ~~(TS//SI//NF)~~

At a minimum, we would have expected the White House to alert Comey directly that it planned to brief the congressional leaders on the Department's position and that it intended to seek Ashcroft's approval of the program despite Comey and Goldsmith's stated legal position against continuing certain activities under the program. Instead, White House officials briefed congressional leaders and sought to have Attorney General Ashcroft recertify the program from his hospital bed without any notice to Comey or anyone else at the Department. We believe these actions gave the appearance of an "end run" around the ranking Justice Department official with whom they disagreed. ~~(TS//SI//NF)~~

C. Recertification of the Presidential Authorization and Modification of the Program (U)

As described in this chapter, the Department had notified Gonzales and Addington of its concerns about the legality of aspects of the program

for several months. In fact, the Department had made clear to the White House in December 2003 and more emphatically in a series of meetings in March 2004 that it believed that aspects of the program could not be legally supported in their existing form. Comey and Goldsmith were clear in their advice to the President and other White House officials. At the hospital, Ashcroft also expressed deep concern [redacted] and told Gonzales and Card that he supported the position of his subordinates. We believe that Ashcroft acted admirably under arduous circumstances. ~~(TS//STLW//SI//OC/NF)~~

Despite the legal concerns uniformly expressed by senior Department of Justice leaders, the White House, through White House Counsel Gonzales, recertified the Authorization, allowing the program to continue substantively unchanged. ~~(TS//SI//NF)~~

Only after Mueller, Comey, and other senior Department and FBI officials made known their intent to resign if the White House continued the program unchanged, despite the Department's conclusion that aspects of the program could not be legally supported, did the President direct that the issue be resolved, and the program be modified to address the Department's legal concerns. Because we were unable to interview key White House officials, we could not determine for certain what caused the White House to change its position and modify the program, although the prospect of mass resignations at the Department and the FBI appears to have been a significant factor in this decision.[233] According to Comey, the President raised a concern that he was hearing about these problems at the last minute, and the President thought it was not fair that he was not told earlier about the Department's legal position. In fact, as Comey informed the President, the President's staff had been advised of these issues "for weeks." ~~(TS//SI//NF)~~

Finally, we believe that the Department and FBI officials who resisted the pressure to recertify the Stellar Wind program because of their belief that aspects of the program were not legally supportable acted courageously and at significant professional risk. We believe that this action by Department and FBI officials – particularly Ashcroft, Comey, Mueller,

---

[233] For instance, we found it significant that on March 16, 2004, White House Counsel Gonzales, who had to make a recommendation to the President about how to proceed with the program in view of the Department's conclusion that legal support for [redacted] called Director Mueller to ask him whether he would resign if the President did not [redacted] Mueller responded that he "would have to give it serious consideration if the President decided to go ahead in the face of DOJ's finding." [redacted] ~~(TS//STLW//SI//OC/NF)~~

Goldsmith, Philbin, and Baker – was in accord with the highest professional standards of the Justice Department. ~~(TS//SI//NF)~~

CHAPTER FIVE
STELLAR WIND PROGRAM'S TRANSITION TO FISA AUTHORITY
(JUNE 2004 THROUGH AUGUST 2007)

In this chapter we examine the transition in stages of the Stellar Wind program from presidential authority to FISA authority. We first describe the FISA Court's approval in July 2004 of the government's application to acquire foreign intelligence information through the collection of bulk e-mail meta data (basket 3 information). This application was based on a legal theory related to FISA's pen register and trap and trace device provisions. We next discuss the government's successful May 2006 application to the FISA Court for an order to obtain bulk telephony meta data (basket 2 information) by the production of business records by certain telecommunications carriers. We then describe the government's interaction with the FISA Court to place under FISA the government's authority to intercept the content of certain communications involving both domestic and foreign telephone numbers and e-mail addresses (basket 1 information). Finally, we summarize legislation enacted in August 2007 and July 2008 to amend FISA to address, among other concerns, the difficulty the government encountered in obtaining FISA authority for content collection, as well as the government's contention that certain provisions of FISA had failed to keep pace with changes in telecommunications technology. ~~(TS//STLW//SI//OC/NF)~~

I. E-Mail Meta Data Collection Under FISA ~~(TS//SI//NF)~~

A. Application and FISA Court Order (U)

[redacted] The FISA Court granted this authority on July 14, 2004 [redacted] ~~(TS//STLW//SI//OC/NF)~~

1. Decision to Seek a Pen Register and Trap and Trace (PR/TT) Order from the FISA Court ~~(TS//SI//NF)~~

[redacted]

[redacted]

Philbin told us that he encountered some opposition to the FISA approach from Counsel to the Vice President David Addington, who argued that the FISA Court was unconstitutional and questioned the need to seek its authorization for e-mail meta data collection. Philbin said that he responded that obtaining an order from the FISA Court was "ironclad safe." Baker recalled attending at least one meeting at the White House with White House Counsel Gonzales and Addington to discuss whether to seek an order from the FISA Court based on FISA's pen register and trap and trace device provisions (a PR/TT Order) and how the FISA Court should be approached to obtain such an order. Baker stated that during the meeting Addington said, "We are one bomb away from getting rid of this obnoxious Court." Baker said Addington also stressed to him that there "is a lot riding on your [Baker's] relationship with this Court." ~~(TS//STLW//SI//OC/NF)~~

In contrast, Hayden told us that he did not have any concerns about transitioning the bulk e-mail meta data collection to FISA authority and was enthusiastic about the move. Hayden stated that while he believed the President had the authority to collect the bulk meta data for the NSA to conduct meta data analysis, he believes that involving an additional branch of government in the activity provided some clarity on this subject. ~~(TS//STLW//SI//OC/NF)~~

Gonzales told us that he did not recall much about the process of filing the application with the FISA Court to obtain e-mail meta data through a PR/TT Order, but stated that there may have been individuals at the White House who expressed concern that seeking the Order from the FISA Court was not a good idea. However, Gonzales told us that he was supportive of seeking the Order [redacted] He stated that he relied on what the intelligence professionals told him and that he would not have supported the PR/TT application if NSA Director Hayden and others did not believe the collection under the PR/TT Order provided the coverage necessary to protect the nation [redacted] Gonzales

also told us that there was concern at the White House that filing the PR/TT application could lead to an unauthorized disclosure of the program. ~~(TS//STLW//SI//OC/NF)~~

2. Briefing for Judge Kollar-Kotelly (U)

In [redacted] Baker, Philbin, and Goldsmith met with Gonzales and Addington at the White House to discuss how to approach Judge Kollar-Kotelly concerning the proposed PR/TT application, and it was decided to give her a "presentation" about the application. The presentation was provided to Judge Kollar-Kotelly on [redacted] Present were Attorney General Ashcroft, Central Intelligence Agency Director George Tenet, FBI Director Mueller, Hayden, Gonzales, OLC Assistant Attorney General Goldsmith, Philbin, Baker, and Director of the Terrorist Threat Integration Center (TTIC) John Brennan. According to an agenda of the briefing, and as confirmed to the OIG, the presentation was given in three parts. First, Mueller, Tenet, and Brennan described the nature of the terrorist threat facing the United States, including concerns of [redacted] Second, Hayden described the technical aspects of the proposed bulk e-mail meta data collection, including how the information was to be collected, archived, queried, and minimized. This portion of the presentation stressed that the NSA required the collection of meta data in bulk to maximize analytic capabilities through contact chaining [redacted] to identify terrorist communications.[234] Third, Philbin explained the government's legal argument that FISA authorized the Court to approve a broad application to collect e-mail meta data under the statute's pen register and trap and trace provisions. ~~(TS//STLW//SI//OC/NF)~~

[redacted] ~~(TS//SI//NF)~~

3. The PR/TT Application ~~(TS//SI//NF)~~

Philbin, Baker, and at least two Office of Legal Counsel attorneys assumed primary responsibility for drafting the PR/TT application to the FISA Court and a memorandum of law in support of the application.[235]

---

[234] The agenda refers to the "needle in haystack" metaphor to illustrate the need for bulk collection, noting "must transform streams of hay into haystack that can later be searched." ~~(TS//SI//NF)~~

[235] The application package, captioned [redacted] consisted of the application; a proposed order authorizing the collection activity and secondary orders mandating carriers to cooperate; a declaration of NSA Director Hayden explaining the technical aspects of the (Cont'd.)

Baker said that Judge Kollar-Kotelly was given a "read-ahead copy" of the application, since it was standard practice to give the FISA Court draft applications for review. ~~(TS//SI//NF)~~

The final application was filed [redacted] A short addendum to the application filed [redacted] it sought authorization from the FISA Court to collect. ~~(TS//SI//NF)~~

The objective of the application was to secure authority under FISA to collect [redacted] bulk e-mail meta data [redacted] the meta data to be collected under FISA authority would be stored in a database. According to the application, queries could be run against the database to identify [redacted] by looking for contacts with other individuals reasonably suspected to be [redacted] and to reveal communications links between such operatives. The resulting analytical products would then be tipped out as leads to the FBI and other elements of the U.S. Intelligence Community to find members of [redacted] disrupt their activities, and prevent future terrorist attacks in the United States.[236] ~~(TS//STLW//SI//OC/NF)~~

The Justice Department constructed its legal argument for this novel use of pen register and trap and trace devices around traditional authorities provided under FISA. Specifically, 50 U.S.C. § 1842(a)(1) authorizes the Attorney General or other designated government attorney to apply

> for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect

---

proposed e-mail meta data collection and identifying the government official seeking to use the pen register and trap and trace devices covered by the application for purposes of 50 U.S.C. § 1842(c)(1); a declaration of Director of Central Intelligence Tenet describing the threat posed by [redacted]; a certification from Attorney General Ashcroft stating that the information likely to be obtained from the pen register and trap and trace devices was relevant to an ongoing investigation to protect against international terrorism, as required by 50 U.S.C. § 1842(c); and a memorandum of law and fact in support of the application. ~~(TS//SI//NF)~~

[236] The application emphasized that Internet e-mail is one of the primary methods by which [redacted] communicate. The memorandum of law in support of the application stated that Internet e-mail is particularly attractive to terrorists [redacted] ~~(TS//SI//NF)~~

> against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order. ~~(TS//SI//NF)~~

FISA incorporated the definitions of the terms "pen register" and "trap and trace device" from 18 U.S.C. § 3127. Thus, FISA adopted as the definition of a "pen register"

> a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication. ~~(TS//SI//NF)~~

18 U.S.C. § 3127(3). FISA also adopted as the definition of a "trap and trace device"

> a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication. ~~(TS//SI//NF)~~

18 U.S.C. § 3127(4).

In its application the government argued that the NSA's proposed collection of meta data met the requirements of FISA by noting that the meta data sought comported with the "dialing, routing, addressing, or signaling information" type of data described in FISA's definitions of pen registers and trap and trace devices. The government also noted that nothing in these definitions required that the "instrument" or "facility" on which the device is placed carry communications of only a single user rather than multiple users. ~~(TS//SI//NF)~~

The government next argued that the information likely to be obtained from the pen register and trap and trace devices was relevant to an ongoing investigation to protect against international terrorism, as certified by the Attorney General under 50 U.S.C. § 1842(c). In support of this "certification of relevance" the government stated that the FBI was conducting more than [redacted] ~~(TS//SI//NF)~~

The government acknowledged that "the overwhelming majority of communications from which meta data will be collected will not be associated with [redacted]." However, the government maintained that FISA did not impose any requirement to tailor collection precisely to obtain only communications that are strictly relevant to the investigation. The government argued that, in any event, "the tailoring analysis must be informed by the balance between the overwhelming national security interest at stake . . . and the minimal intrusion into privacy interests that will be implicated by collecting meta data – especially meta data that will never be seen by a human being unless a connection to a terrorist-associated e-mail is found." ~~(TS//SI//NF)~~

The government also stated that the NSA needed to collect meta data in bulk in order to effectively use analytic tools such as contact chaining [redacted] that would enable the NSA to discover enemy communications. This argument echoed a premise many officials told us about the nature of intelligence gathering in general. For example, Baker likened the search for useful intelligence, particularly in the meta data context, to finding a needle in a haystack, stating, "the only way to find the needle is to have the haystack." Gonzales argued that "to connect the dots you first have to collect the dots." ~~(TS//SI//NF)~~

The application and supporting documents described the [redacted] types of e-mail meta data NSA sought authority to collect:

[redacted]

The application requested that the NSA be authorized to collect this meta data [redacted] were described as follows:

[redacted]

The application represented that for most of the proposed collection on [redacted] it was "overwhelmingly likely" that at least one end of the transmitted communication either originated in or was destined for locations outside the United States, and that in some cases both ends of the communication were entirely overseas.[237] However, the government acknowledged that [redacted] ~~(TS//SI//NF)~~

[redacted]

[237] [redacted]

[redacted]

As discussed below, the government argued and the FISA Court ultimately agreed that the above-described collection [redacted] satisfied the definitions of pen register and trap and trace devices under FISA and Title 18. See 50 U.S.C. § 1841(2); 18 U.S.C. § 3127(3) & (4). ~~(TS//SI//NF)~~

The application also explained the proposed archiving and querying process. According to the application, the collected meta data would be stored in a secure NSA network accessible only through two administrative login accounts and by specially-cleared meta data archive system administrators. Each time the database was accessed, the retrieval request would be recorded for auditing purposes. ~~(TS//SI//NF)~~

The application proposed allowing 10 NSA analysts access to the database.[238] The NSA analysts were to be briefed by the NSA Office of General Counsel concerning the circumstances under which the database could be queried, and all queries would have to be approved by one of seven senior NSA officials.[239] ~~(TS//SI//NF)~~

The application explained that the bulk collection would be queried with particular e-mail addresses in order to conduct chaining [redacted] The application proposed that queries of the e-mail meta data archive would be performed when the e-mail address met the following standard:

> based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known e-mail address is associated with [redacted]

[redacted] Under the PR/TT application, the government proposed that it be authorized under FISA [redacted] to use the reasonable articulable suspicion standard to query the database with specific addressing information [redacted] ~~(TS//STLW//SI//OC/NF)~~

In addition, the NSA proposed applying the minimization procedures in the United States Signals Intelligence Directive 18 (USSID 18) to minimize the information reported concerning U.S. persons. According to the application, compliance with these minimization procedures would be

---

[238] At the government's request the number of NSA analysts was increased to 15 when the Order was renewed [redacted] ~~(TS//SI//NF)~~

[239] When it granted the government's application, the FISA Court noted that in conventional pen register and trap and trace surveillances a court first reviews the application before a particular e-mail account can be targeted. The FISA Court stressed the importance of the NSA Office of General Counsel's obligation to ensure that the legal adequacy for such queries was met. ~~(TS//SI//NF)~~

monitored by the NSA's Inspector General and General Counsel. The government also proposed that in each renewal application the NSA would report to the FISA Court on queries that were made during the prior period and the application of the reasonable articulable suspicion standard for determining that queried addresses were terrorist-related. ~~(TS//SI//NF)~~

The application and supporting documents explained how the NSA intended to use the collected meta data. The NSA sought to use the meta data [redacted] to apply sophisticated algorithms to develop contact chaining [redacted].[240] In the application, the NSA estimated that through external intelligence gathering and internal analysis it would meet the proposed querying standard on average less than once a day. The NSA further estimated that these queries would generate approximately 400 tips to the FBI and CIA per year.[241] Of these tips to the FBI and CIA, the NSA projected that 25 percent would include U.S. person information, amounting to leads including information on about "four to five U.S. persons each month." ~~(TS//SI//NF)~~

4. Judge Kollar-Kotelly Raises Questions about PR/TT Application ~~(TS//SI//NF)~~

On [redacted] Judge Kollar-Kotelly wrote Baker to inform him that she was considering the application and was in the process of preparing an opinion and order in response to it. She wrote that before the opinion and Order could be completed, however, she required written responses to two questions:

(1) Apart from the First Amendment proviso in the statute (50 U.S.C. § 1842(a)(1), (c)(2)), what are the general First Amendment implications of collecting and retaining this large volume of information that is derived, in part, from the communications of U.S. persons?

(2) For how long would the information collected under this authority continue to be of operational value to the counter-terrorism investigation(s) for which it would be collected? ~~(TS//SI//NF)~~

Baker responded in a letter to the FISA Court on [redacted] Concerning the first question, Baker's letter asserted that the proposed

---

[240] These analytic tools are discussed in Chapter Three. (U)

[241] The NSA arrived at this estimate based on the assumption that each query could be expected to generate [redacted] e-mail addresses "one level out," and [redacted] addresses "two levels out." The overall number of direct and indirect contacts with the initial seed address would be significantly reduced using "analytical tradecraft." ~~(TS//SI//NF)~~

collection activity was consistent with the First Amendment and that he could find no reported decisions holding that the use of pen register and trap and trace devices violated the First Amendment. ~~(TS//SI//NF)~~

In his letter, Baker argued that although the meta data collection would include entirely innocent communications, a good-faith investigation does not violate the First Amendment simply because it is "'broa[d] in scope'" (quoting *Laird v. Tatum*, 408 U.S. 1, 10 (1972)). He also wrote that the use of the collected meta data would be "narrowly constrained" because the querying standard for the meta data would be subject to a "reasonable articulable suspicion" of a nexus to [redacted] ~~(TS//SI//NF)~~

Regarding Judge Kollar-Kotelly's second question concerning how long the collected meta data would continue to be of operational value, Baker wrote that, based on the analytic judgment of the NSA, such information would continue to be relevant to [redacted] for at least 18 months. Baker also advised that the NSA believed the e-mail meta data would continue to retain operational value beyond 18 months, but that it should be stored "off-line" and be accessible to queries only by a specially-cleared administrator. Baker proposed that 3 years after the 18-month timeframe, or 4½ years after it is first collected, the meta data could be destroyed.[242] ~~(TS//SI//NF)~~

5. FISA Court Order (U)

In response to the application and follow-up questions, on July 14, 2004, Judge Kollar-Kotelly signed a Pen Register and Trap and Trace Opinion and Order based on her findings that the proposed collection of e-mail meta data and the government's proposed controls over and dissemination of this information satisfied the requirements of FISA. ~~(TS//HCS//SI//NF)~~

The Order granted the government's application in all key respects. It approved for a period of 90 days the collection within the United States of e-mail meta data [redacted] The Order also required the government to comply with certain additional restrictions and procedures either adapted from or not originally proposed in the application. ~~(TS//HCS//SI//NF)~~

In the Order, the Court found that the information to be collected was "dialing, routing, addressing, or signaling information" that did not include

---

[242] On [redacted] the FISA Court issued an order authorizing the NSA to maintain bulk meta data on-line for 4½ years after which time it must be destroyed. According to the NSA Office of General Counsel, the NSA still follows this retention procedure. ~~(TS//HCS//SI//NF)~~

the contents of any communication. The Court stressed that it was only authorizing collection of the [redacted] categories of information delineated in the application, but acknowledged that additional information "could be gleaned" from that meta data, [redacted] The Court found that the means by which the [redacted] categories of meta data were to be collected met the FISA definition of a "pen register," and that the means for collecting the [redacted] category of meta data satisfied the FISA definition of a "trap and trace device." See 18 U.S.C. § 3127(3) & (4), as incorporated in FISA at 50 U.S.C. § 1841(2). ~~(TS//HCS//SI//NF)~~

The Court further found that the government satisfied FISA's requirement that the application certify that the information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism. The Court concluded that, "under the circumstances of this case, the applicable relevance standard does not require a statistical 'tight fit' between the volume of proposed collection and the much smaller proportion of information that will be directly relevant to [redacted] FBI investigations."[243] ~~(TS//HCS//SI//NF)~~

The Court also agreed with the government's position that the privacy interest at stake in the collection of e-mail meta data did not rise to the "stature protected by the Fourth Amendment," and that the nature of the intrusion was mitigated by the restrictions on accessing and disseminating the information, only a small percentage of which would be seen by any person. ~~(TS//HCS//SI//NF)~~

In sum, the Court concluded that the use of pen register and trap and trace devices to collect e-mail meta data would not violate the First Amendment, stating that

> the bulk collection proposed in this case is analogous to suspicionless searches or seizures that have been upheld under the Fourth Amendment in that the Government's need is compelling and immediate, the intrusion on individual privacy interests is limited, and bulk collection appears to be a reasonably effective means of detecting and monitoring [redacted]

---

[243] The Court cautioned that its ruling with regard to the breadth of the meta data collection should not be construed as precedent for similar collections of the full content of communications under the electronic surveillance provisions of FISA. The Court noted important differences in the two types of collection, including the fact that overbroad electronic surveillance requires a showing of probable cause to believe the target is an agent of a foreign power, while the bulk meta data collection under FISA's pen register and trap and trace device provisions merely requires a showing that the overbroad collection is justified as necessary to discover unknown [redacted] persons. The Court also contrasted the high privacy interests at stake with respect to content communications with the absence of a privacy interest in meta data. ~~(TS//SI//NF)~~

[redacted] related operatives and thereby obtaining information likely to be [redacted] to ongoing FBI investigations. ~~(TS//HCS//SI//NF)~~

However, the Court also was concerned that "the extremely broad nature of this collection carries with it a heightened risk that collected information could be subject to various forms of misuse, potentially involving abridgement of First Amendment rights of innocent persons." The Court noted that under 50 U.S.C. § 1842(c)(2), pen register and trap and trace information about the communications of a U.S. person cannot be targeted for collection unless it is relevant to an investigation that is not solely based upon the First Amendment. Therefore, the Court ordered that the NSA modify its criterion for querying the archived data by inserting the following underlined language, as shown below:

> [redacted] will qualify as a seed [redacted] only if NSA concludes, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known e-mail address is associated with [redacted] provided, however, that an [redacted] believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution. ~~(TS//HCS//SI//NF)~~

Regarding the storage, accessing, and disseminating of the e-mail meta data obtained by the NSA, the Court ordered that the NSA must store the information in a manner that ensures it is not commingled with other data, and must "generate a log of auditing information for each occasion when the information is accessed, to include the . . . retrieval request." The Court further ordered that the e-mail meta data "shall be accessed only through queries using the contact chaining [redacted]" as described by the NSA in the government's application. ~~(TS//HCS//SI//NF)~~

The Court noted the "distinctive legal considerations" involved in implementing the authority the Court was vesting in the NSA. Specifically, the Court observed that conventional pen register and trap and trace surveillance required judicial review before any particular e-mail account could be targeted. However, by granting the government's application, the Court noted that the NSA's decision to target an e-mail address (sometimes referred to as a "seed [redacted]") would be made without judicial review. Therefore, the Court ordered that the NSA's Office of General Counsel would be responsible for training analysts to comply with querying standards and

other procedures and "to review the legal adequacy for the basis of such queries, including the First Amendment proviso . . . ." ~~(TS//HCS//SI//NF)~~

As suggested by Baker in his [redacted] response to Judge Kollar-Kotelly's inquiry regarding the useful life of the collected data, the Court ordered that the e-mail meta data shall be available for 18 months for querying. The Court further ordered that after the 18-month period, the data must be transferred to an "off-line" tape system from which it could still be accessed for querying upon approval of the NSA officials authorized to approve queries, and that such meta data must be destroyed 4½ years after initially collected. ~~(TS//HCS//SI//NF)~~

The Court's Order was set to expire after 90 days. The Court required that any application to renew or reinstate the authority granted in the Order must include: a report discussing queries made since the prior application and the NSA's application of the requisite legal standard to those queries; detailed information regarding [redacted] proposed to be added to the authority granted under the Order; any changes to the description of the [redacted] described in the Order or the nature of the communications [redacted]; and any changes to the proposed means of collection, including to the [redacted] of the pen register and trap and trace devices [redacted]
~~(TS//HCS//SI//NF)~~

Finally, the Court issued separate orders [redacted] to assist the NSA with the installation and use of the pen register and trap and trace devices and to maintain the secrecy of the NSA's activities. These orders [redacted] called "secondary orders," [redacted] The NSA was directed to compensate the carriers for all assistance provided in connection with the PR/TT Order.
~~(TS//HCS//SI//NF)~~

Baker and other witnesses told us that obtaining the Order was seen by the Department as a great success, and that there was general agreement that the government had secured all the authority it sought to conduct the bulk e-mail meta data collection. [redacted] Comey told us that obtaining the Order from the FISA Court also provided an "air of legitimacy" to the program.[244] ~~(TS//STLW//SI//OC/NF)~~

[244] Comey and others informally referred to the PR/TT Order as "the mother of all pen registers." ~~(TS//SI//NF)~~

B. President Orders Limited Use [redacted] ~~(TS//STLW//SI//OC/NF)~~

E-mail meta data collection under FISA pen register authority began when the PR/TT Order took effect on July 14, 2004. As required by the Order, the data was placed in its own database or "realm." [redacted]

[redacted]

~~(TS//STLW//SI//OC/NF)~~

We discuss below the President's directive and the OLC memorandum that was drafted to analyze its legality. ~~(TS//STLW//SI//OC/NF)~~

1. The President's August 9, 2004, Memorandum to the Secretary of Defense ~~(TS//SI//NF)~~

On August 9, 2004, the same day a routine Presidential Authorization was issued to continue Stellar Wind, the President sent a separate memorandum to the Secretary of Defense regarding the use of the e-mail meta data collected [redacted] The memorandum directed the Secretary of Defense that, consistent with the August 9, 2004, Presidential Authorization (and any successor Presidential Authorizations), the NSA was authorized to [redacted] e-mail meta data [redacted] when there was a reasonable articulable suspicion that (1) a party to the communication belonged to [redacted] and (2) the purpose of the search was to produce foreign intelligence information concerning threats [redacted][245] ~~(TS//STLW//SI//OC/NF)~~

[245] The President's Memorandum provided that the authority to conduct such searches was to terminate on September 23, 2004. In the September 17, 2004, Presidential Authorization, this authority was extended until November 18, 2004. ~~(TS//STLW//SI//OC/NF)~~

2. Office of Legal Counsel Determines [redacted]

~~(TS//STLW//SI//OC/NF)~~

Jack Goldsmith resigned as Assistant Attorney General for the Office of Legal Counsel on July 30, 2004. Goldsmith was replaced by Daniel Levin, who served as the Acting Assistant Attorney General for OLC until February 2005. (U)

During late 2004, at the request of Comey and Ashcroft, Levin began work on an OLC memorandum addressing whether it would be lawful for the NSA to analyze the e-mail meta data collected [redacted]

~~(TS//STLW//SI//OC/NF)~~ [redacted]

---

246 The [redacted] e-mail meta data has since been placed on tape and is being held by the NSA Office of General Counsel pursuant to a preservation order. ~~(TS//STLW//SI//OC/NF)~~

247 The final version of the OLC memorandum was signed by Levin on February 4, 2005. Levin told the OIG that a "policy decision" was made to limit application of the memorandum to the specific purpose [redacted] However, Levin stated that, based on his analysis of the issue, he believed that [redacted]

(Cont'd.)

Thus, the President asserted extrajudicial authority to order the further use of e-mail meta data collected under Stellar Wind for the limited purpose described in his August 9 memorandum. The FISA Court was notified of this action, although the government did not seek its permission. ~~(TS//STLW//SI//OC/NF)~~

C. Non-Compliance with PR/TT Order ~~(TS//SI//NF)~~

As with other orders issued under FISA, the PR/TT Order was renewed every 90 days. During the early renewals, two major instances of non-compliance were brought to the FISA Court's attention. As described below, these violations of the Order resulted primarily from the NSA senior officials' failure to adequately communicate the technical requirements of the Order to the NSA operators tasked with implementing them, and from miscommunications among the FISA Court, the Justice Department, and the NSA concerning certain legal issues. ~~(TS//SI//NF)~~

1. Filtering Violations ~~(TS//SI//NF)~~

On [redacted] OIPR filed a Notice of Compliance Incidents with the FISA Court. In the Notice, Baker stated that the compliance incidents cited in the Notice "raise compliance issues with about [redacted] of the collection authorized by the Court."[248] The Notice included as an attachment a letter from NSA General Counsel Robert Deitz to Baker describing incidents that led to "unauthorized collection." Deitz learned of these incidents on [redacted].[249] ~~(TS//SI//NF)~~

[redacted]

[redacted] could be queried for any purpose. Levin told us that, other than Addington, no one else was pushing to broaden the memorandum's application. ~~(TS//STLW//SI//OC/NF)~~

[248] Subsequent filings indicate that [redacted] of overall collections under the Order were affected by the violations. ~~(TS//SI//NF)~~

[249] One tipper that was based on this unauthorized collection was disseminated as a lead to the FBI but was subsequently retracted. ~~(TS//SI//NF)~~

[redacted]

(Cont'd.)

[redacted]

Baker told us that Judge Kollar-Kotelly was "not happy" about the violation. On [redacted] the FISA Court issued an Order Regarding [redacted] (Compliance Order). The Court wrote that the "NSA violated its own proposed limitations, which were attested to by its Director and, at the government's invitation, adopted as provisions of the orders of this Court." The Court found that the violations "resulted from deliberate actions by NSA personnel," as distinguished from technical failures. The Court stated it was also troubled by the duration of the violations, which extended from July 14 through [redacted] and that the Court was reluctant to issue a renewal of the PR/TT Order as to [redacted] ~~(TS//SI//NF)~~

That same day, the Court issued an Order to address [redacted] (Order Regarding Required Information for Authorities Involving [redacted], requiring that any application for renewal or reinstatement of PR/TT surveillance authorities [redacted] be accompanied by a sworn declaration by the Secretary of Defense attesting to the state of compliance with the PR/TT Order and a description of the procedures that would be used to ensure compliance. ~~(TS//SI//NF)~~

On [redacted] the government moved for an extension of time (until [redacted]) within which to provide the Secretary of Defense's declaration. The motion, which the Court granted, assured the Court that surveillance [redacted] had been terminated on [redacted] and that on [redacted] the NSA had moved to a separate database all meta data obtained [redacted] through [redacted] The NSA also represented that it reconstructed its contact chaining database using only properly obtained meta data and purged the unauthorized meta data from the system. ~~(TS//SI//NF)~~

A declaration by NSA Director Hayden accompanying the government's motion stated a total of [redacted] e-mail addresses were tipped as leads to the FBI and CIA during the violation period and that [redacted] of these leads may have come from the unauthorized collection. Hayden wrote that

[redacted]

this lead was purged from the FBI's and CIA's databases on [redacted] [redacted] ~~(TS//SI//NF)~~

The NSA Office of the Inspector General subsequently issued a report on its investigation of the unauthorized collections. The NSA OIG report stated that the filtering violations "probably led to actual unauthorized collection, but we have not been able to determine the extent of such collection, and we are not certain that we will be able to do so." The report further stated that the collection program under PR/TT Order authority was [redacted] ~~(TS//STLW//HCS//SI//OC/NF)~~

The report concluded that "there were systemic management failures within both [redacted] within the Signals Intelligence Directorate (SID)], and a complete lack of program management with regard to collection." The report stated that while the training provided by the NSA Office of General Counsel was "vigorous, conscientious, and compliant with the July 14 Order, it was inadequate in scope." ~~(TS//STLW//HCS//SI//OC/NF)~~

According to the report, the NSA removed as much of the tainted collection from the PR/TT database as possible. The NSA was unable to segregate unauthorized collection from [redacted] so it rebuilt that portion of the PR/TT database from [redacted] (the day after the violation was discovered), forward. Moreover, according to the NSA OIG report, analytical personnel were restricted from accessing the unauthorized meta data. ~~(TS//STLW//HCS//SI//OC/NF)~~

2. FISA Court Renews PR/TT Order ~~(TS//SI//NF)~~

The FISA Court's PR/TT Order expired on [redacted] On that date the government filed its first renewal application. The Renewal Application sought authorization to collect e-mail meta data on [redacted] and stated that the NSA had fully complied with the PR/TT Order with respect to [redacted] The government did not seek reauthorization for collection [redacted] due to a variety of operational reasons which the application did not specify. ~~(TS//SI//NF)~~

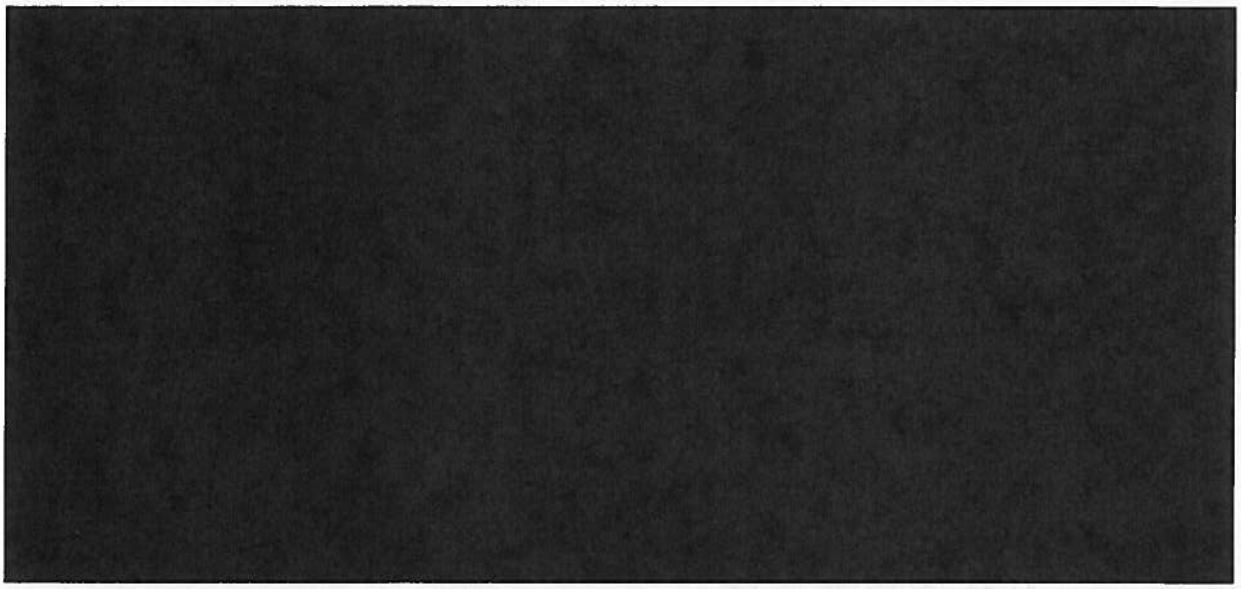
Judge Kollar-Kotelly signed the Renewal Order on [redacted] authorizing through [redacted] the use of pen register and trap and trace devices at [redacted] to collect e-mail meta data. The Renewal Order and the original Order were similar in most respects. However, in the Renewal Order the Court required the NSA to submit reports every 30 days concerning queries made since the prior report and describing any changes made to [redacted] and the [redacted] [redacted].[251] (~~TS//SI//NF~~)

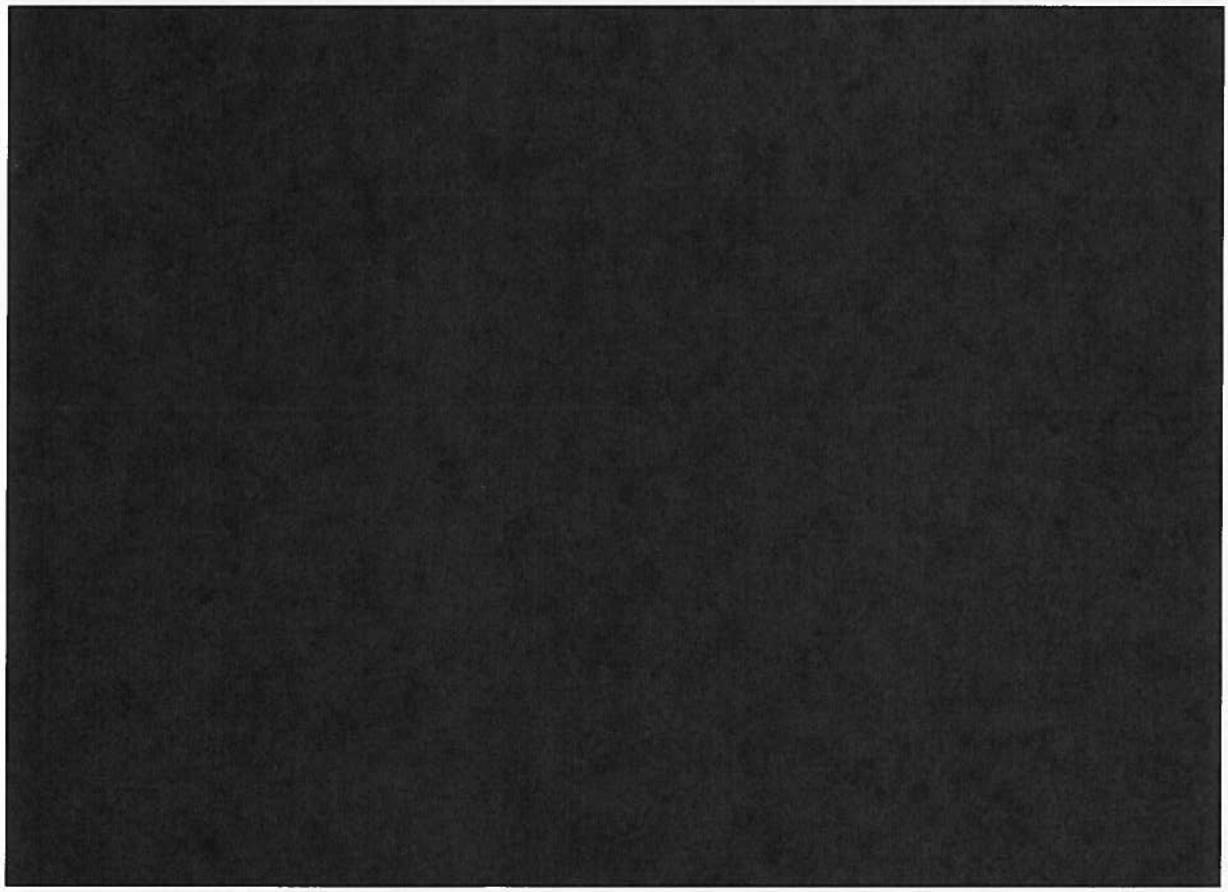
3. [redacted]

Baker told us that during one of his "oversight" visits to the NSA following the FISA Court's PR/TT Order, he was given a demonstration of how the NSA analysts processed the e-mail meta data, including an explanation of how e-mail meta data is collected and queried. Baker said he was informed that among the pieces of data that might be used to meet the reasonable articulable standard for querying the e-mail meta data [redacted] (~~TS//STLW//SI//OC/NF~~) [redacted]

[251] In the initial PR/TT Order, the Court required such a report only upon the government's submission of a renewal application every 90 days. (~~TS//SI//NF~~)

[252] As noted above, seed [redacted] are e-mail addresses or telephone numbers for which a reasonable articulable suspicion exists to believe the [redacted] is related to a terrorist entity. Seed [redacted] are used to query the meta data database to reveal links with other addresses or numbers. (~~TS//SI//NF~~)





[redacted]

D. Subsequent PR/TT Applications and Orders ~~(TS//SI//NF)~~

As described above, the PR/TT Order was first renewed on [redacted] and was renewed by subsequent orders of the FISA Court at approximately 90-day intervals.[254] ~~(TS//SI//NF)~~

On [redacted] the FISA Court issued a Supplemental Order requiring the government to enhance its reporting to the Court of the foreign intelligence benefits realized under the PR/TT Orders. Writing for the FISA Court, Judge Kollar-Kotelly stated that the authority granted under these orders allowed the NSA "to collect vast amounts of information about e-mail [redacted] communications[,]" but that "the Court is unable on the current record to ascertain the extent to which information so collected has actually resulted in the foreign intelligence benefits originally anticipated." Supplemental Order at 1-2. The government responded with a motion requesting that, in light of prior briefings it had given the FISA Court, it not be required to fully comply with the Supplemental Order. It is not clear what if any specific action the FISA Court took in response to this motion, although based on the OIG's review of the PR/TT docket the government continued to submit regular reports to the FISA Court.
~~(TS//STLW//SI//OC/NF)~~

Under the PR/TT renewal applications the scope of authorized queries against the PR/TT database remained limited to queries that concerned [redacted]

[redacted]

[254] In these renewals, [redacted] were added and dropped from [redacted] that were approved in the July 14, 2004, PR/TT Order. ~~(TS//SI//NF)~~

[redacted] ~~(TS//SI//NF)~~

[redacted]

Although the FISA Court continued to renew the NSA's authority to collect and query e-mail meta data, and the NSA proceeded under that authority [redacted] ~~(TS//STLW//SI//OC/NF)~~

II. Telephony Meta Data Collection Under FISA ~~(TS//SI//NF)~~

The second part of the Stellar Wind program brought under FISA authority was the NSA's bulk collection of telephony meta data (basket 2). As described in Chapter Three, under this aspect of the Stellar Wind program the NSA obtained the call detail records of telephone calls, domestic and international [redacted] As with e-mail meta data, the bulk

[redacted]

[257] As discussed in Chapter Three, [redacted] Call detail records consist of routing information, including the originating and terminating telephone number of each call, and the date, time, and duration of each call. The call detail records do not include the substantive content of any communication or the name, address, or financial information of a subscriber or customer. ~~(TS//SI//NF)~~

nature of the telephony collection provided the NSA the ability to conduct [redacted] – contact chaining [redacted] ~~(TS//STLW//SI//OC/NF)~~

The transition of bulk telephony meta data collection from Presidential Authorization under the Stellar Wind program to FISA authority relied on a provision in the FISA statute that authorized the FBI to seek an order from the FISA Court compelling the production of "any tangible things" from any business, organization, or entity, provided the items are for an authorized investigation to protect against international terrorism or clandestine intelligence activities. See 50 U.S.C. § 1861. Orders under this provision commonly are referred to as "Section 215" orders in reference to Section 215 of the USA PATRIOT ACT, which amended the "business records" provision in title V of FISA.[258] The "tangible things" the government sought in the Section 215 application described in this section were the call detail records [redacted]. ~~(TS//STLW//SI//OC/NF)~~

We describe below the circumstances that led to the government's decision to transition the bulk collection of telephony meta data from presidential authority to FISA Authority. We then summarize the government's initial application and the related Court Order. ~~(TS//STLW//SI//OC/NF)~~

A. Decision to Seek Order Compelling Production of Call detail records ~~(TS//SI//NF)~~

The timing of the Department's decision in May 2006 to seek a FISA Court order for the bulk collection of telephony meta data was driven primarily by external events. On December 16, 2005, The New York Times published an article entitled, "Bush Lets U.S. Spy on Callers Without Courts." The article, which we discuss in more detail in Chapter Eight, described in broad terms the content collection aspect of the Stellar Wind program, stating that the NSA had "monitored the international telephone calls of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible 'dirty numbers' linked to al Qaeda." [redacted] ~~(TS//STLW//SI//OC/NF)~~

[258] The term "USA PATRIOT Act" is an acronym for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). It is commonly referred to as "the Patriot Act." (U)

On December 17, 2005, in response to the article, President Bush publicly confirmed that he had authorized the NSA to intercept the international communications of people with "known links" to al Qaeda and related terrorist organizations (basket 1). On January 19, 2006, the Justice Department issued a document entitled "Legal Authorities Supporting the Activities of the National Security Agency Described by the President" and informally referred to as a "White Paper," that addressed in an unclassified form the legal basis for the collection activities that were described in the New York Times article and confirmed by the President. ~~(TS//STLW//SI//OC/NF)~~

According to Steven Bradbury, the head of OLC at that time, the legal analysis contained in the White Paper [redacted] Although the New York Times article did not describe this aspect of Stellar Wind, reporters at USA Today were asking about this aspect of the program in early 2006. Bradbury [redacted] anticipated that a USA Today story would attract significant public attention when it was published.[259] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[259] On May 11, 2006, USA Today published the results of its investigation. The article, entitled "NSA Has Massive Database of American Phone Calls," reported that the NSA "had been secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon, and BellSouth." The article stated that the program, launched shortly after the September 11 attacks, collected the records of billions of domestic calls in order to analyze calling patterns to detect terrorist activity. The article reported that the records provided to the NSA did not include customer names, street addresses, and other personal information, but noted that such information was readily available by cross-checking the telephone numbers against other databases. ~~(TS//STLW//I//OC/NF))~~

[redacted]

[redacted]

B. Summary of Department's Application and Related FISA Court Order ~~(S/NF)~~

As noted previously, applications to the FISA Court that seek an order compelling the production of "tangible things" are commonly referred to as "Section 215" applications, in reference to Section 215 of the USA PATRIOT ACT. Section 215 authorizes the FBI to request a FISA Court order

> requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution. (U)

50 U.S.C. § 1861(a)(1).[261] Section 215 does not require that the items sought pertain to the subject of an investigation; the government need only demonstrate that the items are relevant to an authorized investigation.[262] (U)

On May 23, 2006, the FBI filed with the FISA Court a Section 215 application seeking authority to collect telephony meta data to assist the NSA in finding and identifying known and unknown members or agents of [redacted] in support of the [redacted] related FBI investigations then pending and other Intelligence Community operations. The application requested an order compelling [redacted] to produce (for the duration of the 90-day order) call detail records relating to all telephone communications maintained by the carriers. The application described call detail records as routing information that included the

---

[261] "United States person" is defined in FISA as a citizen, legal permanent resident, or unincorporated association in which a "substantial number" of members are citizens or legal permanent residents, and corporations incorporated in the United States as long as such associations or corporations are not themselves "foreign powers." 50 U.S.C. § 1801(i)(2005). (U)

[262] Prior to the enactment of Section 215, the FISA statute's "business records" provisions were limited to obtaining information about a specific person or entity under investigation. Also, information could be obtained only from common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities. (U)

originating and terminating telephone number of each call, and the date, time, and duration of each call. The application stated that telephony meta data did not include the substantive content of any communication or the name, address, or financial information of a subscriber or customer. According to the application, the majority of the telephony meta data provided to the NSA was expected to involve communications that were (1) between the United States and abroad, or (2) wholly within the United States, including local telephone calls. [redacted].[263] ~~(TS//SI//NF)~~

The application acknowledged that the [redacted] collection would include records of communications of U.S. persons located within the United States who were not the subject of any FBI investigation. However, relying on the precedent established by the PR/TT Order, the application asserted that the collection was needed for the NSA to perform analysis to find known [redacted] and to identify unknown operatives, some of whom may be in the United States or in communication with U.S. persons. The application stated that it was not possible to determine in advance which particular piece of meta data will identify a terrorist. The application stated that obtaining such bulk data increases the NSA's ability, through contact-chaining [redacted] to detect and identify members of [redacted].[264] In other words, according to the application, meta data analysis is possible only if the NSA "has collected and archived a broad set of metadata that contains within it the subset of communications that can later be identified as terrorist-related."[265] ~~(TS//SI//NF)~~

---

[263] The NSA told us that the actual average amount of telephony meta data collected per day is approximately [redacted] call detail records and that the figure has not reached [redacted] ~~(TS//SI//NF)~~

[264] [redacted]

[265] The FISA Court had stated in its July 2004 PR/TT Order that the FISA statute's "relevance" requirement is a relatively low standard and that in evaluating whether bulk meta data is "relevant" to an investigation into [redacted] "deference should be given to the fully considered judgment of the executive branch in assessing and responding to national security threats and in determining the potential significance of intelligence-related information." The government cited this precedent in the Section 215 application, stating, "[j]ust as the bulk collection of e-mail meta data was relevant to FBI investigations into [redacted] so is the bulk collection of telephony metadata described herein." ~~(TS//SI//NF)~~

The application also explained how the meta data would be used. [redacted] [266] The database could be queried only if the NSA determined that, "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [redacted] the Section 215 application, like the PR/TT application and Order, added the following proviso to the query standard: "provided, however, that a telephone number believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution." ~~(TS//SI//NF)~~

According to the application, the NSA estimated that only a tiny fraction (1 in 4 million, or 0.000025 percent) of the call detail records included in the database were expected to be analyzed. The results of any such analysis would be provided, or "tipped," to the FBI or other federal agencies (as was being done under Stellar Wind). [redacted] ~~(TS//SI//NF)~~

The application also proposed restrictions on access to, and the processing and dissemination of, the data collected that were essentially identical to those included in the PR/TT Order. These included the requirement that queries be approved by one of seven NSA officials or managers and that the NSA's Office of the General Counsel would review and approve proposed queries of telephone numbers reasonably believed to be used by U.S. persons.[267] ~~(TS//SI//NF)~~

[266] [redacted]

[267] The application included several other measures to provide oversight of the use of meta data, such as controls on the dissemination of any U.S. person information, the creation of a capability to audit NSA analysts with access to the meta data, the destruction of collected meta data after a period of 5 years (the destruction period for e-mail meta data was 4½ years), and a review by the NSA's Inspector General and General Counsel conducted within 45 days of implementing the FISA Court order that assessed the

(Cont'd.)

On May 24, 2006, the FISA Court approved the Section 215 application. The Court's Order stated that there were reasonable grounds to believe that the telephony meta data records sought were relevant to authorized investigations being conducted by the FBI to protect against international terrorism. The Order incorporated each of the procedures proposed in the government's application relating to access to and use of the meta data. These procedures included a requirement that any application to renew or reinstate the authority for the bulk collection contain a report describing (1) the queries made since the Order was granted; (2) the manner in which the procedures relating to access and use of the meta data were applied; and (3) any proposed changes in the way in which the call detail records would be received from the communications carriers. The Order also requires the Justice Department to review, at least every 90 days, a sample of the NSA's justifications for querying the call detail records. ~~(TS//SI//NF)~~

Through March 2009, the FISA Court renewed the authorities granted in the May 24 Order at approximately 90-day intervals, with some modifications sought by the government. For example, the Court granted a motion filed on August 8, 2006, requesting [redacted] 268 [redacted] Except for these and other minor modifications, the terms of the FISA Court's grant of Section 215 authority for the bulk collection of telephony meta data remained essentially unchanged since first approved on May 24, 2006, through March 2009. [redacted] Further, the FISA Court's Section 215 Orders did not require the NSA to modify its use of the telephony meta data from an analytical perspective. However, as discussed below, the FISA Court drastically changed the authority contained in its March 2009 Section 215 Order following the government's disclosure of incidents involving the NSA's failure to comply with the terms of the Court's prior orders. ~~(TS//STLW//SI//OC/NF)~~

---

adequacy of the management controls for the processing and dissemination of U.S. person information. ~~(TS//SI//NF)~~

268 As noted above, the Court granted an identical motion at the same time in connection with the bulk collection of e-mail meta data. ~~(TS//SI//NF)~~

C. Non-Compliance with Section 215 Orders ~~(TS//SI//NF)~~

On January 9, 2009, representatives from the Department's National Security Division attended a briefing at the NSA concerning the telephony meta data collection. During the course of this briefing, and as confirmed by the NSA in the days that followed, the Department came to understand that the NSA was querying the telephony meta data in a manner that was not authorized by the FISA Court's Section 215 Orders. Specifically, the NSA was on a daily basis automatically querying the meta data with thousands of telephone identifiers from an "alert list" that had not been determined to satisfy the reasonable articulable suspicion (RAS) standard the Court required be met before the NSA was authorized to "access the archived data" for search or analysis purposes.[269] ~~(TS//SI//NF)~~

The alert list contained telephone identifiers that were of interest to NSA counterterrorism analysts responsible for tracking the targets of the Section 215 Orders [redacted] The list was used to compare the incoming telephony meta data obtained under FISA authority, [redacted] Under the procedures the NSA had developed to implement the Section 215 authority, alerts (or matches) generated from RAS-approved identifiers could be used to automatically conduct contact chaining [redacted] of the telephony meta data. However, automated analysis for alerts generated by non-RAS approved identifiers were not permitted; instead, the alerts were sent to analysts to determine whether chaining [redacted] was warranted in accordance with the RAS standard. ~~(TS//SI//NF)~~

On January 15, 2009, the Justice Department notified the FISA Court that the NSA had been accessing the telephony meta data with non-RAS approved identifiers. [redacted].[270] On January 28, 2009, the

---

[269] The term "telephone identifier" used by the government means a telephone number as well as other unique identifiers associated with a particular user or telecommunications device for purposes of billing or routing communications. ~~(TS//SI//NF)~~

[270] Following the Department's notice to the Court, the NSA attempted to complete a software fix to the alert process so that "hits" against the telephony meta data generated by non-RAS-approved telephone identifiers were deleted and that only "hits" generated by RAS-approved identifiers were sent to NSA analysts for further analysis. The NSA also attempted to construct a new alert list consisting of only RAS-approved telephone identifiers. However, the implementation of these modifications was unsuccessful and on January 24, 2009, the NSA shut down the alert process completely. ~~(TS//SI//NF)~~

Court issued an order stating that it was "exceptionally concerned about what appears to be a flagrant violation of its Order in this matter[.]" The Court required the government to file a brief to "help the Court assess whether the Orders in this docket should be modified or rescinded; whether other remedial steps should be directed; and whether the Court should take action regarding persons responsible for any misrepresentations to the Court or violation of its Orders, either through its contempt powers or by referral to appropriate investigative offices." The Court also required the government to address several additional specific issues, including who knew that the alert list being used to query the meta data included identifiers that had not been determined to meet the reasonable and articulable suspicion standard, how long the "unauthorized querying" had been conducted, and why none of the entities the Court directed to conduct reviews of the meta data collection program identified the problem earlier.[271] ~~(TS//SI//NF)~~

On February 17, 2009, the government responded to the Court's Order and acknowledged that the NSA's previous descriptions to the Court of the alert list process were inaccurate and that the Section 215 Order did not authorize the government to use the alert list in the manner that it did. The government described for the Court in detail how the NSA developed procedures in May 2006 to implement the Section 215 authority that resulted in the NSA querying the telephony meta data with non-RAS approved telephone identifiers for over 2 years in violation of the Court's Orders, and how those procedures came to be described incorrectly to the Court. According to the government, the situation resulted from the NSA's interpretation of the term "archived data" used in the Court's Orders and the NSA's mistaken belief that the alert process under the Section 215 authority operated the same as the alert process under the Pen Register/Trap and Trace authority.[272] The government told the Court that "there was never a complete understanding among key personnel" who reviewed the initial report to the Court describing the alert process about

---

[271] The entities directed to conduct such reviews under the Section 215 Orders were the NSA's Inspector General, General Counsel, and Signals Intelligence Directorate Oversight and Compliance Office. (U//~~FOUO~~)

[272] The NSA understood the term "archived data" in the Court's Order to refer to the NSA's analytical repository for the telephony meta data. As the term is normally used by [redacted] The NSA believed that the requirement to satisfy the RAS standard was only triggered when the NSA sought access to the stored, or "archived," repository of telephony meta data. For this reason, in the NSA's view, it was not required to limit the alert list to RAS-approved identifiers. ~~(TS//SI//NF)~~

what certain terminology was intended to mean, and that "there was no single person who had complete technical understanding of the BR FISA system architecture." ~~(TS//SI//NF)~~

The government argued that the Section 215 Orders should not be rescinded or modified "in light of the significant steps that the Government has already taken to remedy the alert list compliance incident and its effects, the significant oversight modifications the Government is in the process of implementing, and the value of the telephony metadata collection to the Government's national security mission[.]"[273] Among the several measures the government highlighted to the Court was the NSA Director's decision to order "end-to-end system engineering and process reviews (technical and operational) of NSA's handling of [telephony] metadata." Less than two weeks after the government filed the response summarized above, the government informed the Court that the NSA had identified additional compliance incidents during these reviews.[274] ~~(TS//SI//NF)~~

In Orders dated March 2 and 5, 2009, the FISA Court addressed the compliance incidents reported by the government and imposed drastic changes to the Section 215 authorities previously granted. The Court first addressed the NSA's interpretation of the term "archived data." The Court said the interpretation "strains credulity" and observed that an interpretation that turns on whether the meta data being accessed has been "archived" in a particular database at the time of the access would "render compliance with the RAS requirement merely optional." ~~(TS//SI//NF)~~

---

[273] [redacted] The NSA also determined that in all instances that a U.S. telephone identifier was used to query the meta data for a report, the identifier was either already the subject of a FISA Court order or had been reviewed by the NSA's Office of General Counsel to ensure the RAS determination was not based solely on a U.S. person's First Amendment-protected activities. ~~(TS//SI//NF)~~

[274] The additional compliance incidents involved the NSA's handling of the telephony meta data in an unauthorized manner. The first incident involved the NSA's use of an analytical tool to query (usually automatically) the meta data with non-RAS approved telephone identifiers. The tool determined if a record of a telephone identifier was present in NSA databases and, if so, provided analysts with information about the calling activity associated with that identifier. The second incident involved three analysts who conducted chaining analyses in the telephony meta data using 14 non-RAS approved identifiers. According to the government's notice to the Court, the analysts conducted queries of non-FISA authorized telephony meta data and were unaware their queries also ran against the FISA-authorized meta data. The government stated that none of the queries used an identifier associated with a U.S. person or telephone identifier and none of the queries resulted in intelligence reporting. ~~(TS//SI//NF)~~

The Court next addressed the misrepresentations the government made to the Court from August 2006 to December 2008 in reports that inaccurately described the alert list process. The Court recounted the specific misrepresentations and summarized the government's explanation for their occurrence. The Court then concluded,

> Regardless of what factors contributed to making these misrepresentations, the Court finds that the government's failure to ensure that responsible officials adequately understood the NSA's alert list process, and to accurately report its implementation to the Court, has prevented, for more than two years, both the government and the FISC from taking steps to remedy daily violations of the minimization procedures set forth in FISC orders and designed to protect [redacted] call detail records pertaining to telephone communications of U.S. persons located within the United States who are not the subject of any FBI investigations and whose call detail information could not otherwise have been legally captured in bulk. ~~(TS//SI//NF)~~

The Court also addressed the additional non-compliance incidents that were identified during the initial review ordered by the NSA Director, observing that the incidents occurred despite the NSA implementing measures specifically intended to prevent their occurrence. In view of the record of compliance incidents the government had reported to date, the Court stated,

> [I]t has finally come to light that the FISC's authorizations of this vast collection program have been premised on a flawed depiction of how the NSA uses BR metadata. This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall BR regime has never functioned effectively. ~~(TS//SI//NF)~~

Despite the Court's concerns with the telephony meta data program, and its lack of confidence "that the government is doing its utmost to ensure that those responsible for implementation fully comply with the Court's orders," it authorized the government to continue collecting telephony meta data under the Section 215 Orders. The Court explained that in light of the

government's repeated representations that the collection of the telephony meta data is vital to national security, taken together with the Court's prior determination that the collection properly administered conforms with the FISA statute, "it would not be prudent" to order the government to cease the bulk collection. ~~(TS//SI//NF)~~

However, believing that "more is needed to protect the privacy of U.S. person information acquired and retained" pursuant to the Section 215 Orders, the Court prohibited the government from accessing the meta data collected "until such time as the government is able to restore the Court's confidence that the government can and will comply with previously approved procedures for accessing such data."[275] The government may, on a case-by-case basis, request authority from the Court to query the meta data to obtain foreign intelligence.[276] Such a request must specify the telephone identifier to be used and the factual basis for the NSA's RAS determination. ~~(TS//SI//NF)~~

The Court ordered that upon completion of the NSA's end-to-end system engineering and process reviews, the government file a report that describes the results of reviews, discusses the steps taken to remedy non-compliance incidents, and proposes minimization and oversight procedures to employ should the Court authorize resumption of regular access to the telephony meta data. The government's report also must include an affidavit from the FBI Director and any other government national security official deemed appropriate describing the value of the telephony meta data to U.S. national security. ~~(TS//SI//NF)~~

Additionally, the Court ordered the government to implement oversight mechanisms proposed in the government's response to the compliance incidents. These mechanisms generally require the Justice Department's National Security Division to assume a more prominent role in the NSA's administration of the bulk collection program. For example, the NSA's Office of General Counsel must now consult with the National

---

[275] The Court also stated, "Given the Executive Branch's responsibility for and expertise in determining how best to protect our national security, and in light of the scale of this bulk collection program, the Court must rely heavily on the government to monitor this program to ensure that it continues to be justified, in the view of those responsible for our national security, and that it is being implemented in a manner that protects the privacy interests of U.S. persons[.]" ~~(TS//SI//NF)~~

[276] The Court authorized the government to query the meta data without Court approval to protect against an imminent threat to human life, with notice to the Court within the next business day of the query being conducted. The Court also authorized the government to access the meta data to ensure "data integrity" and to develop and test technological measures designed to enable to the NSA to comply with previously approved procedures for accessing the meta data. ~~(TS//SI//NF)~~

Security Division on all significant legal opinions that relate to the interpretation, scope, or implementation of past, current, and future Section 215 Orders related to the telephony bulk meta data collection. ~~(TS//SI//NF)~~

On May 29, 2009, the Court authorized the government to continue collecting telephony meta data under the Section 215 Orders for 43 days subject to the same limitations set out in its orders of March 2 and 5, 2009. ~~(TS//SI//NF)~~

III. Content Collection under FISA ~~(TS//SI//NF)~~

The third and last part of the Stellar Wind program brought under FISA authority was content collection (basket 1). The effort to accomplish this transition was legally and operationally complex, and our discussion in this section does not address each statutory element or the full chronology of the government's applications and related FISA Court orders. Rather, we describe the circumstances surrounding the government's decision to transition content collection from presidential to FISA authority [redacted] We also summarize the FISA Court's response to the government's content collection proposals and the orders it issued. In this section, we describe one FISA Court judge's rejection of the government's legal approach to content collection, a decision that hastened the enactment of legislation that significantly amended the FISA statute and provided the government surveillance authorities broader than those authorized under Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

A. Decision to Seek Content Order ~~(TS//SI//NF)~~

The Department first began work on bringing Stellar Wind's content collection activity (basket 1) under FISA in March 2005, shortly after Alberto Gonzales became Attorney General. Gonzales told us that he initiated discussions about making this change with OLC Principal Deputy Assistant Attorney General Bradbury. Gonzales said that he had questions about how the NSA was conducting the collection in terms of audits and checks being performed, and he wanted to ensure that the agency was running the program properly. Gonzales told us that placing content collection under FISA authority would also eliminate the constitutional debate about the activity and would reassure people that the President was acting according to the Constitution and the law. Gonzales said that, in his view, it is better to conduct activities such as content collection without a direct order from the President when possible. Gonzales added that in 2001 nobody thought it was possible to bring Stellar Wind under FISA authority. ~~(TS//STLW//SI//OC/NF)~~

When Gonzales became Attorney General in early 2005, however, he also knew there had been a leak to The New York Times about the NSA's content collection activity under Stellar Wind and that the paper was actively investigating the story. In November 2004, Gonzales (then the White House Counsel), together with Deputy Attorney General Comey and his Chief of Staff, had met with New York Times reporters to discuss the potential article.[277] ~~(TS//STLW//SI//OC/NF)~~

In response to Gonzales's request, Bradbury, working with attorneys in OLC and the Office of Intelligence and Policy Review (OIPR) as well as with NSA personnel, devised a legal theory, summarized below, for bringing under FISA the Stellar Wind program's content collection activities while preserving the "speed and agility" many Intelligence Community officials cited as the chief advantage of the NSA program. In June 2005, Bradbury, together with Associate Deputy Attorney General Patrick Philbin, presented the legal theory to White House officials David Addington, Harriet Miers, and Daniel Levin and received their approval to continue work on a draft FISA application.[278] ~~(TS//STLW//SI//OC/NF)~~

Bradbury told the OIG that he also spoke to the Director of National Intelligence and to NSA officials about bringing Stellar Wind's content collection under FISA. According to Bradbury, the Director of National Intelligence responded positively to the proposal, but the NSA was skeptical as to whether a FISA approach would be feasible, in view of the substantial administrative requirements under the FISA Court's PR/TT Order. The NSA also believed that the FISA Court would be reluctant to grant the NSA the operational flexibility it would insist on in any content application, resulting in less surveillance coverage of telephone numbers and e-mail addresses used by persons outside the United States. ~~(TS//STLW//SI//OC/NF)~~

As discussed in detail in Chapter Eight of this report, in December 2005 The New York Times published its series of articles on the content collection portion of the Stellar Wind program, resulting in considerable controversy and public criticism of the NSA program. Through the spring of 2006, the Department continued work on the content application. In May 2006, at the first of the FISA Court's semiannual meetings that year, the Department provided the Court a draft of the application for content collection to obtain feedback on the government's unconventional approach to the FISA statute. None of FISA Court judges indicated whether the

---

[277] The New York Times held the article until December 2005, when it published a series of articles on the content collection portion of Stellar Wind. ~~(TS//SI//NF)~~

[278] After serving as Acting Assistant Attorney General for OLC from June 2004 to February 2005, Levin joined the National Security Council, where he remained until approximately November 2005. (U)

application would be granted if filed, but some identified concerns with certain aspects of the proposal. ~~(TS//STLW//SI//OC/NF)~~

At this time, Congress and the Administration were also discussing how to modernize the FISA statute to authorize the type of electronic surveillance that the content application sought. Work on the application was temporarily suspended as the Department focused its attention on working with Congress to craft this legislation. However, this suspension of work on the content application was brief. Bradbury said he concluded by the fall of 2006, as Congress was heading for recess, that there would be no legislative reform of the FISA statute in the foreseeable future that would address content collection as it was being conducted under Stellar Wind. As a result, the Department pressed forward with the draft content application to the FISA Court. ~~(TS//STLW//SI//OC/NF)~~

B. Summary of Department's December 13, 2006, Content Application ~~(TS//SI//NF)~~

In November 2006, at the second of the Court's semiannual meetings, the Department presented an updated draft of the application that incorporated feedback received from members of the Court during the previous semiannual meeting. On December 13, 2006, the Department formally filed the content application with the Court. ~~(TS//SI//NF)~~

The government's December 13 application sought authority to intercept the content of telephonic and electronic communications of [redacted].[279] The application stated:

> Speed and flexibility are essential in tracking individuals who [redacted] To follow the trails effectively, and to respond to new leads, it is vital for the U.S. Intelligence Community to be able quickly and efficiently to acquire communications to or from individuals reasonably believed to

[279] The content application included the following caveat:

> By filing this application, the United States does not in any way suggest that the President lacks constitutional or statutory authority to conduct the electronic surveillance detailed herein without Court authorization. ~~(TS//SI//NF)~~

be members or agents of these [redacted] foreign powers. ~~(TS//SI//NF)~~

According to the application, the goal was to establish "an early warning system" under FISA to alert the government to the presence of members and agents of foreign powers [redacted] and to assist tracking such individuals within the United States. The "early warning system" sought to replace the conventional practice under FISA of filing individual applications each time the government had probable cause to believe that a particular phone number or e-mail address, referred to by the NSA as a "selector," was being used or about to be used by members or agents of a foreign power. ~~(TS//SI//NF)~~

In the place of this individualized process, the application proposed that the FISA Court establish broad parameters for the interception of communications – specifically, [redacted] that can be targeted and the locations where the surveillance can be conducted – and that NSA officials, rather than FISA Court judges, determine within these parameters the particular selectors whose communications the NSA would intercept. [redacted] albeit with FISA Court review and supervision.[280] ~~(TS//SI//NF)~~

The legal arguments underlying the government's approach are complex and involve substantial communications terminology. They also require lengthy discussion of the FISA statute and previous FISA Court decisions. Rather than describe at length these issues, in this section we detail the two main components of the government's approach to content collection in the FISA application that are critical for understanding one judge's approval of the application and another judge's later rejection of essentially the same application. ~~(TS//SI//NF)~~

First, the government proposed an interpretation of the term "facility" in the FISA statute that was broader than how the term was ordinarily, but

---

[280] The Department's application provided an example to illustrate the risks associated with the existing requirement that FISA Court approval or Attorney General emergency authorization be obtained each time the government seeks to target a particular telephone number or e-mail address: [redacted] According to the application, valuable intelligence could be lost in the time it would take to receive FISA Court authorization or Attorney General emergency authorization to target the new address. ~~(TS//SI//NF)~~

not always, applied.[281] Section 1805(a)(3)(B) of FISA provides that the Court may order electronic surveillance only upon finding that there is probable cause to believe that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by" a group involved in international terrorism. The term "facilities" generally was interpreted to refer to individual telephone numbers or e-mail addresses at which surveillance is "directed." ~~(TS//SI//NF)~~

The government proposed in its content application that the term "facilities" be interpreted broadly to include [redacted][282] Under this approach, instead of examining the target's use of particular telephone numbers or e-mail addresses, the Court would determine only whether there was probable cause to believe that the target was using [redacted] to communicate telephonically or by e-mail.[283] ~~(TS//STLW//SI//OC/NF)~~

Second, the government's application requested that senior NSA officials be authorized to make individualized findings of probable cause about whether a particular telephone number or e-mail address was being used by a member or agent of one of the application's targets. Ordinarily, a FISA Court judge makes this probable cause determination. ~~(TS//SI//NF)~~

To implement this transfer of authority, the government proposed that NSA officials make the probable cause determinations as part of requirements called "minimization procedures," which are detailed rules

---

[281] The government's Memorandum of Law filed in support of the content application described several instances where the FISA Court authorized surveillance of facilities that was not limited to particular telephone numbers and e-mail addresses. According to the application [redacted] The government's proposed interpretation of the term in the content application was far broader than previously authorized by the Court. ~~(TS//SI//NF)~~

[282] [redacted]

[283] As noted, the targets of the content application were [redacted] The government's content application included a declaration from the NSA Director that addressed [redacted] use of the international telephone system and [redacted] communications. ~~(TS//SI//NF)~~

that govern how the government must handle communications that it intercepts pertaining to U.S. persons. The FISA statute provides that each FISA application must include, and the FISA Court must approve, minimization procedures that the agency will follow with respect to communications intercepted pursuant to a FISA Court order. ~~(TS//SI//NF)~~

Minimization procedures, in the FISA context, ordinarily govern the handling of intercepted communications involving U.S. persons after the acquisition has been approved by the FISA Court. In other words, a FISA Court authorizes the agency to intercept the communications of particular selectors, and the agency follows the minimization procedures with respect to how it retains, uses, and disseminates any U.S. person information it collects under the Court's order. ~~(TS//SI//NF)~~

However, the government proposed as part of the content application that the minimization procedures also encompass how the NSA acquires the communications.[284] Specifically, the application proposed that the NSA could intercept the communications of specific selectors if agency officials determined there was probable cause to believe that (1) the selector is being used by a member or agent of a [redacted] and (2) the communication is to or from a foreign country. The application referred to this as the "minimization probable cause standard."[285] ~~(TS//SI//NF)~~

Thus, the content application had a two-prong "minimization probable cause standard": (1) probable cause to believe a selector is being used by a member or agent of a targeted group, and (2) probable cause to believe the communication intercepted is to or from a foreign country. [redacted]

---

[284] Bradbury told the OIG that this argument was based on the text of the FISA statute, which states that minimization procedures apply to the "acquisition" of communications in addition to their retention and dissemination. See 50 U.S.C. § 1801(h)(1). Indeed, the government's Memorandum of Law filed in support of the content application described several cases in which the FISA Court authorized the government to conduct electronic surveillance that included minimization at the time of acquisition. According to the application, the cases involved surveillance broadly targeted [redacted] than those the government specifically sought to acquire. [redacted] ~~(TS//SI//NF)~~

[285] The proposed "minimization probable cause standard" was in addition to the standard minimization procedures that accompany every FISA application submitted by the government and that have been long-approved by the FISA Court. ~~(TS//SI//NF)~~

[redacted] ~~(TS//STLW//SI//OC/NF)~~

For the first prong – probable cause to believe a selector is being used by a member or agent of a targeted group – NSA analysts would assess sources of "reliable intelligence," defined in the application as information from a variety of domestic and foreign intelligence and law enforcement activities. Under the terms of the application, positive findings of probable cause would be recorded in a database and the assessment process would be subject to periodic internal review by NSA officials, including the NSA General Counsel and Inspector General. ~~(TS//SI//NF)~~

For the second prong – probable cause to believe the communication intercepted is to or from a foreign country [redacted] For example, the application stated that there would be probable cause to believe [redacted]

[redacted] [286] With respect to e-mails, the application stated that [redacted]

[redacted] [287] ~~(TS//STLW//SI//OC/NF)~~

---

[286] The application acknowledged that communications intercepted at the "facilities" could include some calls where [redacted] in the United States, or where [redacted] in the United States (even where there is probable cause to believe that [redacted] the United States). [redacted] If the NSA had probable cause to believe one of the communicants was a member of [redacted] the call could be intercepted. The application stated that such communications would be handled in accordance with NSA's standard minimization procedures that apply to all of the agency's electronic surveillance activities. ~~(TS//SI//NF)~~

[287] As it did with telephone communications, the application acknowledged that the manner in which e-mail communications are routed would cause the NSA to collect some e-mail communications that in fact are between communicants wholly within the United (Cont'd.)

Thus, viewing the government's approach to both "facilities" and "minimization procedures" together, the December 13, 2006, content application asked the FISA Court to find probable cause to believe that [redacted] engaged in international terrorism, and that these groups use the international telephone system and the [redacted] communications system [redacted] Then, within these broad parameters authorized by the Court, NSA officials would make probable cause findings about whether individual telephone numbers or e-mail addresses are used by members or agents of [redacted] and whether the communications of those numbers and addresses are to or from a foreign country. If they were, the NSA could direct the telecommunications carriers to intercept the communications of those telephone numbers and e-mail addresses and provide them to the NSA. [redacted] ~~(TS//STLW//SI//OC/NF)~~

Under the terms of the application, communications acquired by the NSA could be retained for 5 years, unless the Court approved retention for a longer period. The application also stated that the NSA expected to initially target [redacted] telephone numbers and e-mail addresses used by members or agents or [redacted] ~~(TS//SI//NF)~~

An additional aspect of the content application is important to understand. The "early warning system" the government proposed applied both to "domestic selectors" and "foreign selectors." Domestic selectors are telephone numbers and e-mail addresses reasonably believed to be used by individuals in the United States; foreign selectors are telephone numbers and e-mail addresses reasonably believed to be used by individuals outside the United States. Under Stellar Wind, the NSA intercepted the communications of both categories of selectors, although the NSA tasked far more foreign selectors than domestic selectors. ~~(TS//STLW//SI//OC/NF)~~

States, even though the NSA had probable cause to believe the communication was to or from a foreign country. The application stated that the NSA would handle any such communications in accordance with its standard minimization procedures. ~~(TS//SI//NF)~~

The government proposed in its content application that the domestic selectors would be subject to more rigorous targeting approval and more frequent reporting to the FISA Court than foreign selectors, but the application sought to preserve NSA officials' authority to make the probable cause determinations as to each.[288] As we describe below, the first FISA Court judge to consider the content application, Judge Malcolm Howard, was unwilling to extend this authority to domestic selectors. ~~(TS//SI//NF)~~

C. Judge Howard Grants Application in Part ~~(TS//SI//NF)~~

The Department's December 13, 2006, content application was assigned to Judge Howard, because he was the "duty" judge that week responsible for considering new applications.[289] Judge Howard advised the Department orally that he would not authorize, on the terms proposed in the application, the electronic surveillance of selectors to be used by persons in the United States (domestic selectors). He did not issue a written opinion or order concerning this decision. The Department, in response to Judge Howard's oral advisement, filed a separate application requesting authority to conduct electronic surveillance on domestic selectors. This application, summarized below, was filed on January 9, 2007, and is considered the first "domestic selectors application"; the December 13 application is considered the first "foreign selectors application." ~~(TS//SI//NF)~~

Judge Howard also requested additional briefing from the Justice Department on the subject of whether [redacted] constituted "facilities" under FISA, and whether the surveillance authority sought in the government's content application would in fact be "directed" not at these "facilities" but rather at the particular telephone numbers and e-mail addresses the government would task for collection. ~~(TS//SI//NF)~~

In response, the Department filed a supplemental memorandum of law on January 2, 2007, arguing that the government's construction of the

---

[288] Under the terms of the original content application, domestic selectors tasked by the government would subsequently be reported to the Court for approval. The Court either had to approve each domestic selector within 48 hours of receiving the government's report or, if the Court did not agree there was probable cause to believe the selector was being used by a member or agent of a target of the application, provide the government 24 hours to submit additional information establishing probable cause. Foreign selectors tasked by the government did not require subsequent approval by the Court, although the Court could direct that the surveillance of any selector cease. ~~(TS//SI//NF)~~

[289] The Department offered to submit the application to the FISA Presiding Judge, Judge Kollar-Kotelly, but she said that it should be filed in the normal fashion, which meant it would be assigned to the FISA duty judge that week. ~~(TS//SI//NF)~~

terms "facilities" and "directed" was fully consistent with the text of FISA and supported by FISA Court practice and precedent. The memorandum further explained why the traditional approach to surveillance under FISA would not provide the speed and agility necessary for the "early warning system" the application sought to create.[290] ~~(TS//SI//NF)~~

On January 10, 2007, Judge Howard approved the Department's content application as to foreign selectors, endorsing the legal framework on which the content application for foreign selectors was based, including the broad construction of the term "facility" and the use of minimization procedures to empower NSA officials to make targeting decisions about particular selectors. Judge Howard's Order authorized the government to conduct electronic surveillance for a period of 90 days at the "facilities" identified in the application, and was set to expire on April 6, 2007. The Order [redacted].[291] ~~(TS//SI//NF)~~

Judge Howard's Order also required that an attorney from the Justice Department's National Security Division review the NSA's justifications for targeting particular foreign selectors. The Order required the government to submit reports to the FISA Court every 30 days listing new selectors tasked during the previous 30 days and briefly summarizing the basis for the NSA's determination that the first prong of the minimization probable cause standard has been met for each new selector.[292] The Order preserved the Court's authority to direct that surveillance cease on any selectors for which

---

[290] On this point, the memorandum cited the government's limited resources as presenting a significant obstacle to filing a separate FISA application for each selector it wanted to place under surveillance. The government stated that it anticipated initiating collection on [redacted] new selectors each month, a figure that translates to filing a motion to amend a FISA order or seeking Attorney General emergency authority [redacted] times per day (or, alternatively, filing one motion or seeking one Attorney General emergency authorization covering [redacted] new selectors each day). The government stated that if the government proceeded under any of these options, valuable intelligence would be lost. ~~(TS//SI//NF)~~

[291] As noted earlier, the Order compelled [redacted]. The Order also required that with each request for reauthorization, the government present a list of current selectors previously reported to the Court that the government intended to continue tasking, identify any selectors reasonably believed to be used by U.S. persons outside the United States, and assess the efficacy of the collection of communications that mentioned a tasked e-mail address [redacted] but that were not to or from that selector. ~~(TS//SI//NF)~~

[292] As noted above, the first prong of the standard is probable cause to believe that the selector is being used by a member or agent of a targeted [redacted]. ~~(TS//SI//NF)~~

the Court found that the first prong of the standard has not been satisfied. In addition, the Order required the NSA Inspector General, General Counsel, and Signals Intelligence Directorate to periodically review the authorized collection activities. These NSA offices were required to submit a report to the Court 60 days after the collection was initiated under the Order that would address the adequacy of management controls and whether U.S. person information was being handled properly. ~~(TS//SI//NF)~~

According to several Department and NSA officials, the effort to implement Judge Howard's January 10, 2007, Order was a massive undertaking. [redacted] ~~(TS//STLW//SI//OC/NF)~~

As a result of the Order, the Department and NSA submitted to the FISA Court for its review the factual basis for each selector supporting the government's determination that the "minimization probable cause standard" had been satisfied. The Department accomplished this pursuant to a schedule approved by Judge Howard under which the Department filed [redacted] foreign selectors every [redacted] days for the duration of the 90-day Order. ~~(TS//SI//NF)~~

The probable cause explanation for each foreign selector filed with the Court typically was described in several sentences. According to Bradbury, he impressed upon the NSA that Judge Howard would review each submission and inquire about how recently the NSA had acquired communications relating to a particular selector. According to Matthew Olsen, the Deputy Assistant Attorney General in the Department's National Security Division who was responsible for overseeing intelligence matters, Judge Howard did in some cases inquire about the government's factual basis for believing the minimization probable cause standard has been met.[293] Bradbury also said he stressed that the Court would scrutinize the NSA's probable cause determinations more rigorously than the agency had been doing itself and that the Court was more likely to approve a selector where the surveillance was current than it would a selector that has "remained dormant for months."[294] ~~(TS//SI//NF)~~

---

[293] Olsen was involved in the drafting and presentation to the FISA Court of the content application and the government's implementation of the related FISA Court Orders. ~~(TS//SI//NF)~~

[294] However, Bradbury noted that the FISA Court's "tendency to look for recent information" in assessing whether the probable cause standard has been met is "problematic" because [redacted]

(Cont'd.)

Olsen told us that [redacted] foreign selectors ultimately were filed with the FISA Court under the terms of Judge Howard's Order. Olsen said that the NSA strived to submit selectors that were deemed high priority, that had a well-documented nexus to [redacted] foreign powers, and that had recent communications activity. Attorneys from OIPR, who under the terms of the Order were required to review the NSA's justification for each foreign selector that it tasked, worked with the NSA on this large-scale review process. According to Olsen, OIPR attorneys "double-checked" the NSA's probable cause determination for each selector, but did not conduct independent probable cause inquiries. This review identified [redacted] selectors that in OIPR's judgment required additional documentation before they could be submitted to the Court.[295] Olsen described the back-and-forth between OIPR and the NSA as "constant," and said the NSA was receptive to OIPR's involvement. Olsen stated that the NSA committed significant resources to the transition of foreign selectors. ~~(TS//SI//NF)~~

Both Bradbury and Olsen observed that the transition of content collection of foreign selectors to FISA required some adjustment by the NSA in its approach to establishing probable cause. For example, while an NSA analyst might base a probable cause determination to some extent on intuition, similar to a "cop on the beat," it was a different proposition when that probable cause determination had to be reviewed by several OIPR attorneys trying to anticipate how the FISA Court might view the judgment. Olsen stated that it was also "new" for the NSA to document the probable cause to the level OIPR believed the FISA Court would require. According to Bradbury, the effort sought an equilibrium between "the necessary speed and agility" and the "multiple layers of probable cause determination." Bradbury and Olsen both told the OIG that the NSA had concerns about whether the FISA approach to content collection would work and the extent to which a measure of effectiveness would be lost under FISA Court supervision. ~~(TS//SI//NF)~~

D. Domestic Selectors Application and Order ~~(TS//SI//NF)~~

In contrast to foreign selectors, Judge Howard advised the Justice Department that requests for surveillance of the international calls of domestic selectors – telephone numbers or e-mail addresses reasonably believed to be used by individuals in the United States – should be filed with

[redacted] ~~(TS//SI//NF)~~

[295] Olsen told the OIG that he believes the NSA de-tasked some of these foreign selectors. ~~(TS//SI//NF)~~

the Court in a separate application. Judge Howard also advised OIPR officials that any such application should take a more traditional approach to FISA, meaning the "facilities" targeted by the application should be particular telephone numbers and e-mail addresses and that the probable cause determination for tasking a selector would reside with the FISA Court, not with NSA officials pursuant to minimization procedures. ~~(TS//SI//NF)~~

On January 9, 2007, the Department filed the first domestic selectors application. The application sought two things. First, the application requested authority to intercept the international communications of [redacted] specific domestic selectors.[296] Second, the application sought, for purposes of future applications, approval to use a "streamlined version" of the emergency authorization procedures available under FISA. These emergency procedures authorize the use of electronic surveillance for a period of up to 72 hours without a Court order when the Attorney General reasonably determined that an emergency situation exists. See 50 U.S.C. § 1805(f). The procedures required the Attorney General to inform the FISA Court that the surveillance has been initiated and required the Department to file with the Court an emergency application to continue the surveillance not more that 72 hours after the surveillance was authorized. ~~(TS//SI//NF)~~

The goal of the Department's proposed streamlined emergency application procedures, referred to in the January 9, 2007, application as a "Verified Application," was to ensure that the emergency surveillance process be completed as swiftly as possible for qualifying domestic selectors. The proposal allowed the Verified Application to incorporate by reference the reasons or facts contained in the original domestic selectors application necessary to satisfy some of the statutory requirements under FISA, instead of reestablishing in each application for a new domestic selector that each of the requirements of FISA were met. The only new substantive information contained in a Verified Application would be the identity of the target, if known, the telephone number the target was using or was about to use, and the factual basis supporting probable cause to believe the target is [redacted] and is using or is about to use the identified telephone number. ~~(TS//SI//NF)~~

Judge Howard granted the domestic selectors application on January 10, 2007, for a period of 90 days. His Order also approved the

---

[296] Unlike the December 13, 2006, application, the January 9, 2007, application did not seek authority to target agents of [redacted] nor did the application seek authority to conduct content surveillance of e-mail communications. The declaration summarized for each of the domestic selectors, generally in two to three paragraphs, the facts that supported the government's belief that the telephone number was used or about to be used by a known or unknown agent of [redacted] located in the United States. ~~(TS//SI//NF)~~

streamlined emergency authorization procedures proposed in the application for any additional domestic selectors whose communications the government sought to intercept during the 90-day period for which surveillance was authorized.[297] ~~(TS//SI//NF)~~

NSD Deputy Assistant Attorney General Olsen told the OIG that in comparison with foreign selectors, the Department conducted a more rigorous review of the initial domestic selectors submitted to the FISA Court to ensure that probable cause was met. Olsen said a few domestic selector packages "on [their] face" lacked sufficient documentation and that these deficiencies were apparent to OIPR attorneys reviewing the information because the attorneys were looking at the information for the first time. He said that the NSA analysts responsible for the selectors, in contrast, were very familiar with the numbers and knowledgeable of details about the users that might not have been evident to persons reviewing documentation *de novo*. According to Olsen, for selector packages that were considered deficient, the NSA either provided the Justice Department attorneys with additional information or de-tasked the selector.[298] ~~(TS//SI//NF)~~

E. Last Stellar Wind Presidential Authorization Expires ~~(TS//SI//NF)~~

On December 8, 2006, the President signed what would become the final Presidential Authorization for the Stellar Wind program. The December 8 Authorization was scheduled to expire on February 1, 2007. However, Judge Howard's January 10, 2007, Orders relating to foreign and domestic selectors completed the transition of Stellar Wind's

---

[297] On January 22, 2007, the Department filed, and Judge Howard approved, the first Verified Application with the FISA Court using the streamlined procedures approved in the Order. ~~(TS//SI//NF)~~

[298] Olsen and OIPR Deputy Counsel Margaret Skelly-Nolen told the OIG that during the application for and implementation of the domestic selectors Order, it became apparent that there were coordination problems between the FBI and the NSA. They noted that in many instances a domestic selector the NSA sought to task was already targeted by an FBI FISA order. According to Skelly-Nolen, in those cases problems can arise in providing accurate, current, and consistent information to the FISA Court about such selectors. She said the NSA's practice has been to consult with the FBI analysts assigned to the NSA and to request from them the most current information the FBI has about a particular telephone number or user of that number. The FBI analysts at the NSA have access to FBI databases to search for such information, although the most current information frequently can only be obtained from the operational personnel at FBI Headquarters. As a consequence, according to Skelly-Nolen, the FISA Court has on some limited occasions been provided inconsistent information concerning domestic telephone numbers or the users of those numbers. Olsen told the OIG that the domestic selectors Order has required a higher level of coordination between the FBI and NSA and that the National Security Division has worked to address this issue. ~~(TS//SI//NF)~~

communications and meta data collection activities from Presidential Authorization to FISA authority. Bradbury told the OIG that because it was believed that Judge Howard's Orders, particularly the foreign selectors Order, provided the NSA sufficient flexibility to conduct content collection, it was not necessary to renew the December 8, 2006, Presidential Authorization. ~~(TS//STLW//SI//OC/NF)~~

Therefore, on February 1, 2007, the Presidential Authorization for the Stellar Wind program officially expired.[299] ~~(TS//SI//NF)~~

F. First Domestic and Foreign Selectors FISA Renewal Applications ~~(TS//SI//NF)~~

Judge Howard's January 10, 2007, Orders were set to expire after 90 days. During the week of March 20, 2007, the government filed renewal applications to extend the authorities both as to domestic and foreign selectors. These applications were filed with Judge Roger Vinson, the FISA Court duty judge that week. ~~(TS//SI//NF)~~

The domestic selectors application, filed March 22, 2007, was in all material respects identical to the government's original application. Judge Vinson granted the application on April 5, 2007.[300] ~~(TS//SI//NF)~~

The foreign selectors application was filed on March 20, 2007. The content and construction of the March 20 application was substantially identical to the government's original application, and advanced the same broad construction of the term "facilities" and the use of minimization procedures to authorize NSA officials, instead of judges, to make probable cause determinations (subsequently reviewed by the FISA Court) about particular selectors. ~~(TS//SI//NF)~~

On March 29, 2007, Judge Vinson orally advised the Department that he could not grant the foreign selectors application. His decision validated some concerns within the Justice Department that Judge Howard's original

---

[299] On January 17, 2007, Attorney General Gonzales sent a letter to Senators Leahy and Specter, the Chairman and Ranking Member of the Senate Judiciary Committee, informing them of Judge Howard's Orders. Gonzales's letter stated that as a result of the January 10, 2007, FISA Court Orders, any electronic surveillance that was occurring under the Terrorist Surveillance Program would now be conducted under FISA, and that "the President determined not to reauthorize the Terrorist Surveillance Program when the current authorization expires." ~~(TS//SI//NF)~~

[300] As noted previously, the domestic selectors Order presented special coordination issues between the FBI and the NSA, and [redacted] The Order was renewed for the final time in [redacted] and has since expired. ~~(TS//SI//NF)~~

Order might not be a sustainable long-term strategy for intercepting the communications of foreign selectors. Judge Vinson's decision also accelerated the Department's efforts to obtain legislation amending the FISA statute to authorize the type of surveillance conducted under Stellar Wind and that was approved by Judge Howard. ~~(TS//SI//NF)~~

On April 3, 2007, Judge Vinson issued an Order and Memorandum Opinion explaining the reasoning for his conclusion that he could not grant the foreign selectors application. However, Judge Vinson did not deny the government's application. Instead, he encouraged the Department to file a motion with Judge Howard requesting a 60-day extension of the existing January 10, 2007, foreign selectors Order. In explaining why he was encouraging the Department of file the motion with Judge Howard, Judge Vinson wrote,

> I have concluded that an extension for this purpose is appropriate, in view of the following circumstances: that the government has commendably devoted substantial resources to bring the NSA's surveillance program, which had been conducted under the President's assertion of non-FISA authorities, within the purview of FISA; that a judge of this Court previously authorized this surveillance in [the January 10, 2007, foreign selectors Order], on substantially the same terms as the government now proposes; that it would be no simple matter for the government to terminate surveillance of [redacted] phone numbers and e-mail addresses under FISA authority, and to decide whether and how it should continue some or all of the surveillance under non-FISA authority; and, importantly, that within the allotted time the government may be able to submit an application that would permit me to authorize at least part of the surveillance in a manner consistent with this order and opinion. ~~(TS//SI//NF)~~

Judge Vinson wrote that the Department's foreign selectors renewal application concerns an "extremely important issue" regarding who may make probable cause findings that determine the individuals and the communications that can be subjected to electronic surveillance under FISA. In Judge Vinson's view, the question was whether probable cause determinations are required to be made by the FISA Court through procedures established by statute, or whether the NSA may make such determinations under an alternative mechanism cast as "minimization procedures." Judge Vinson concluded, based on past practice under FISA and the congressional intent underlying the statute, that probable cause determinations must be made by the FISA Court. ~~(TS//SI//NF)~~

In explaining his reasoning, Judge Vinson first rejected the Department's broad construction of the term "facilities," concluding that the "electronic surveillance" under the government's application – the acquisition of the content of communications – was directed at particular telephone numbers and e-mail addresses, and not at broad swaths of communications [redacted], as the government contended. Judge Vinson distinguished prior cases that the government cited for its broad interpretation of "facilities," observing, "[t]ellingly, none of the cited cases stand for the proposition on which this application rests – that electronic surveillance is not 'directed' at particular phone numbers and e-mail addresses, [redacted]." ~~(TS//SI//NF)~~

Judge Vinson wrote that his conclusion was also supported by the government's and the Court's past practice, as well as the legislative history of FISA, which, according to Judge Vinson, made clear that "Congress intended the pre-surveillance 'judicial warrant procedure,' and particularly the judge's probable cause findings, to provide an 'external check' on executive branch decisions to conduct surveillance." He wrote that the government's proposal that "the Court assess [redacted] and make a highly abstract and generalized probable cause finding [redacted]" removed from the Court's pre-surveillance purview the question of whether the communications to be acquired will relate to the targeted foreign powers.[301] ~~(TS//SI//NF)~~

Judge Vinson rejected the government's "minimization probable cause standard," stating that "[m]inimization does not provide a substitute for, or a mechanism for overriding, the other requirements of FISA." Judge Vinson concluded that government's proposed minimization procedures, by authorizing the NSA to make probable cause decisions, conflicted with specific provisions of FISA that govern electronic surveillance, such the requirement that only the Attorney General can grant emergency approvals to conduct surveillance (followed within 72 hours by an application to the

---

[301] Stated another way, "[the application] represented that NSA will make the required probable cause finding for each such facility before commencing surveillance." Judge Vision wrote, "[t]he application seeks, in effect, to delegate to the NSA the Court's responsibility to make such findings 'based on the totality of circumstances.' Obviously, this would be inconsistent with the statutory requirement and the congressional intent that the Court make such findings prior to issuing the order (emphasis in original)." ~~(TS//SI//NF)~~

FISA Court), and that renewals for surveillance coverage must be based on "new findings" of probable cause by a judge. Judge Vinson summarized his position:

> The clear purpose of these statutory provisions is to ensure that, as a general rule, surveillances are supported by judicial determinations of probable cause before they commence; that decisions to initiate surveillance prior to judicial review in emergency circumstances are made at politically accountable levels; that judicial review of such emergency authorizations follows swiftly; and that decisions to continue surveillance receive the same degree of scrutiny as decisions to initiate. The law does not permit me, under the rubric of minimization, to approve or authorize alternative procedures to relieve the government of burdensome safeguards expressly imposed by the statute. ~~(TS//SI//NF)~~

Judge Vinson wrote that he was mindful of the government's argument that the proposed minimization procedures were necessary to provide or enhance the "speed and flexibility" with which the NSA responds to threats, and that foreign intelligence information may be lost in the time it takes to obtain Attorney General emergency authorizations. However, in Judge Vinson's view, FISA's requirements reflected a balance struck by Congress between privacy interests and the need to obtain foreign intelligence information, and until Congress took legislative action on FISA to respond to the government's concerns, the Court must apply the statute's procedures.[302] He concluded that the government's application sought to strike a different balance for the surveillance of foreign telephone numbers and e-mail addresses. Vinson rejected this position, stating, "provided that the surveillance is within FISA at all, the statute applies the same requirements to surveillance of facilities used overseas as it does to surveillance of facilities used in the United States."[303] ~~(TS//SI//NF)~~

---

[302] Judge Vinson stated that he recognized that the government maintained the President may have constitutional or statutory authority to conduct the surveillance requested in the renewal application. Judge Vinson stated, "[n]othing in this order and opinion is intended to address the existence or scope of such authority, or this Court's jurisdiction over such matters." ~~(TS//SI//NF)~~

[303] Judge Vinson wrote in a footnote that the status of the proposed surveillance as being within the scope of FISA was "assumed, but not decided, for purposes of this order and opinion." He continued, "I believe that there are jurisdictional issues regarding the application of FISA to communications that are between or among parties who are all located outside the United States." Judge Vinson suggested that "Congress should also consider clarifying or modifying the scope of FISA and of this Court's jurisdiction with regard to such facilities . . . ." Bradbury told the OIG that Judge Vinson's suggestion was an important spur to Congress's willingness to consider FISA modernization legislation in

(Cont'd.)

Attorney General Gonzales told us that his reaction to Judge Vinson's decision was one of "disappointment" and that the decision "confirmed our concern about going to the [FISA Court]." Gonzales also said he believed the decision was "troubling for purposes of the national security of our country." ~~(TS//STLW//SI//OC/NF)~~

Bradbury told us the government considered several options after Judge Vinson's ruling, including appealing the decision to the FISA Court of Review. However, he said the decision was made to attempt to work with Judge Vinson to craft a revised application and also separately to renew the Administration's efforts to obtain legislation to modernize FISA. ~~(TS//SI//NF)~~

G. Revised Renewal Application for Foreign Selectors and Order ~~(TS//SI//NF)~~

As suggested by Judge Vinson, in April 2007 the Justice Department obtained from Judge Howard an extension of the existing foreign selectors Order until May 31, 2007, to prepare a revised foreign selectors application. In the interim, the Department filed two reports with Judge Vinson describing a new approach to foreign selectors that addressed the concerns expressed in his Opinion, and that sought input from the Court about how best to facilitate the submission of an application that would seek authority to direct surveillance at [redacted] selectors. ~~(TS//SI//NF)~~

On May 24, 2007, the Department filed a revised renewal application seeking to renew, with modifications, the authorities granted in Judge Howard's January 10, 2007, Order. However, the application did not include the broad construction of "facilities" and instead sought authority to conduct electronic surveillance of conventional facilities – telephone numbers and "e-mail [redacted]."[304] The application also did not include the "probable cause minimization standard" approved

---

the summer of 2007. In Section IV below, we summarize this legislation, the Protect America Act, and its successor, the FISA Amendments Act of 2008. ~~(TS//SI//NF)~~

[304] According to the May 24, 2007, application, such uses include Internet communications that are sent to and from a targeted e-mail "address," [redacted] The May 24 application was the [redacted] to use the term "e-mail [redacted]" to describe the facility at which e-mail surveillance would be directed; [redacted] However, according to the application, the government "routinely requests, and the Court authorizes, electronic surveillance using [the e-mail [redacted]] descriptor to identify this type of facility." ~~(TS//STLW//SI//OC/NF)~~

by Judge Howard that had the effect of shifting from the FISA Court to the NSA the probable cause determinations about particular selectors. ~~(TS//SI//NF)~~

However, the targets of the government's revised application remained selectors (telephone number and e-mail facilities) reasonably believed to be used outside the United States and for which there is probable cause to believe were being used, or are about to be used, by [redacted]

[redacted] [305] The application also sought [redacted] and in the same manner as was approved in Judge Howard's Order.[306] ~~(TS//SI//NF)~~

Specifically, the application requested authority to direct surveillance at [redacted] categories of foreign selectors:

- Foreign telephone number and e-mail selectors presently known to the government. This category accounted for a portion of the [redacted] foreign selectors already under surveillance pursuant to Judge Howard's Order.[307]

[redacted]

[305] The May 24, 2007, application explicitly stated that the government was not seeking surveillance authority for any new facilities reasonably believed by the NSA to be used by U.S. persons. The application stated that surveillance of those facilities would be initiated only through FISA's emergency authorization provisions and the streamlined FISA applications approved for domestic selectors. ~~(TS//SI//NF)~~

[306] [redacted]

[307] The government submitted an appendix with the revised renewal application that identified [redacted] facilities and contained the factual basis for the NSA's belief that each of the facilities was being used by a person outside the United States and for which there was probable cause to believe were being used or about to be used by a member or agent of one of the targeted foreign powers. The government had provided Judge Vinson these facilities on a rolling basis during May 2007 for his consideration. The NSA discontinued the surveillance of facilities that were targeted under Judge Howard's Order, but that were not included among the facilities submitted to Judge Vinson for approval. The NSA told the OIG that the decision to discontinue surveillance on these [redacted] facilities largely was a resource decision and that [redacted] facilities figure was the amount the NSA could timely process for filing with the Court. ~~(TS//SI//NF)~~

[redacted]

- Foreign e-mail selectors (not telephone number selectors) presently unknown to the government but that "refer to" or are "about" known foreign e-mail selectors. This category of surveillance, which the NSA had been conducting under Judge Howard's Order, includes situations where an already targeted e-mail facility is mentioned in the body of a message between two third-party, non-targeted facilities.[308] ~~(TS//SI//NF)~~

According to the application, the [redacted] of surveillance would enable the NSA to initiate surveillance of newly discovered facilities "with the speed and agility necessary to obtain vital intelligence and to detect and prevent terrorist attacks." The application stated,

[redacted]

The collection authorities requested in the renewal application that pertained to currently unknown facilities would, according to the application, address this limitation.[309] ~~(TS//SI//NF)~~

Judge Vinson granted the government's revised renewal application on May 31, 2007. His Order authorized, for a period of 90 days, each of the [redacted] categories of electronic surveillance described above, although the

---

[308] The category presented an issue under FISA in that communications are being acquired because they contain the targeted e-mail selector, and not because there was probable cause to believe the e-mail accounts sending or receiving the communications are used or about to be used by an international terrorist group. In such cases, the surveillance is not "directed at" the targeted e-mail selector. The government argued that such acquisition was still consistent with FISA because, "at the time of acquisition, the NSA has probable cause to believe that the facilities at which the NSA is directing surveillance are being used by the foreign power target." ~~(TS//SI//NF)~~

[309] The government argued that the FISA Court's authority to authorize subsequent collection against new selectors unknown to the government at the time an application was approved is rooted in section 1805(c)(3) of FISA. That provision imposes specific reporting requirements on the government where the FISA Court approves an electronic surveillance in circumstances where the nature and location of each of the facilities at which surveillance will be directed is unknown at the time of the application. ~~(TS//SI//NF)~~

Order defined the precise circumstances under which the NSA could acquire communications falling within the [redacted] category of surveillance.[310] The Order also included reporting schedules with respect to the [redacted] categories of surveillance, for which the government was required to submit newly discovered selectors to the Court. ~~(TS//SI//NF)~~

Judge Vinson initially approved [redacted] foreign selectors under the terms of his May 31, 2007, Order (these selectors were submitted with the government's May 24, 2007, application). Shortly after the Order was issued, the FISA Court decided that the weekly reports filed by the government notifying the Court of newly discovered selectors, as well as the government's motions seeking approval to conduct surveillance on additional selectors, could be filed for review with any member of the Court. As the government received feedback from judges on the first reports and motions that were filed, it observed that judges were applying a more rigorous standard of review to the factual basis supporting the surveillance for each selector than Judge Vinson applied to the [redacted] selectors he approved. The government consequently adjusted the amount of factual information it provided the FISA Court in subsequent reports and motions and ultimately added [redacted] foreign selectors to Judge Vinson's Order. ~~(TS//SI//NF)~~

According to Bradbury, the more rigorous scrutiny applied by FISA Court judges after Judge Vinson's initial approval [redacted] foreign selectors caused the NSA place only a fraction of the foreign selectors under coverage than it wanted to. This concern, combined with the comparatively laborious process for targeting foreign selectors under Judge Vinson's Order, accelerated the government's efforts to obtain legislation that would amend FISA to address the government's surveillance capabilities within the United States directed at persons located outside the United States. The Protect America Act, signed into law on August 5, 2007, accomplished this objective

---

[310] [redacted] However, his Order authorized the surveillance of any previously non-targeted e-mail facilities that transmitted e-mail messages containing a targeted e-mail account only when the NSA determined, based on the acquired communication and other intelligence or publicly available information, that there was probable cause to believe the e-mail facility was being used, or was about to be used, by one of the targeted foreign powers. Judge Vinson agreed with the government's position that there was probable cause to believe that Internet communications relating to a previously targeted e-mail facility were themselves being sent or received by one of the targeted foreign powers and could be acquired. Judge Vinson called this holding "novel," but concluded that the decision was "consistent with the overall statutory requirements; it requires the government to promptly report and provide appropriate justification to the Court; and it supplies the Government with a necessary degree of agility and flexibility in tracking the targeted foreign powers." ~~(TS//SI//NF)~~

and effectively superseded Judge Vinson's foreign selectors Order. The government therefore did not seek to renew the Order when it expired on August 24, 2007. ~~(TS//SI//NF)~~

In the next section, we summarize the effect of the Protect America Act and successor legislation, the FISA Amendments Act of 2008. (U)

IV. The Protect America Act and the FISA Amendments Act of 2008 (U)

In August 2007, the Protect America Act was enacted, amending FISA to address the government's ability to conduct electronic surveillance in the United States of persons reasonably believed to be located outside the United States. This legislation expired on February 1, 2008, but was extended by Congress to February 16, 2008. In July 2008, the FISA Amendments Act of 2008 was enacted, which, among other things, created a comprehensive process under FISA for content collection directed at foreign targets. These two laws modernized the FISA statute as it applied to the acquisition in the United States of communications of persons reasonably believed to be outside the United States. (U)

As discussed in Chapter Three, FISA was enacted in 1978 when most international calls were carried by satellite. The interception of such calls constituted "electronic surveillance" for purposes of FISA only if the acquisition intentionally targeted a U.S. person in the United States, or if all participants to the communication were located in the United States. Thus, government surveillance of satellite communications that targeted foreign persons outside the United States generally was not considered electronic surveillance, and the government was not required to obtain a FISA Court order authorizing the surveillance even if one of the parties to the communication was in the United States. However, in the mid-1980s, fiber optic technology began to replace satellites as the primary means for transmitting international (and domestic) telephone communications. This change brought within FISA's definition of "electronic surveillance" the acquisition of telephone calls to or from a person in the United States if the acquisition occurred in the United States, thereby triggering the requirement that the government obtain FISA Court orders to conduct surveillance that it previously conducted outside of FISA. ~~(TS//SI//NF)~~

Under the Stellar Wind program, the NSA collected international communications [redacted] by targeting facilities (telephone numbers and e-mail addresses) located outside the United States (foreign

selectors).[311] As noted in Chapters Three and Four, the Administration contended that FISA, as supplemented by a subsequent legislative enactment (the AUMF), did not preclude the surveillance activities under Stellar Wind, or in the alternative represented an unconstitutional infringement on the President's Article II authority as Commander in Chief to the extent it conflicted with these collection activities. ~~(TS//STLW//SI//OC/NF)~~

The Justice Department's effort to transfer content collection from presidential authority under Stellar Wind to FISA raised the issue of FISA's application to the acquisition in the United States of communications to or from targeted foreign selectors. The Protect America Act and the FISA Amendments Act, in slightly different ways, addressed this issue by treating the communications of persons reasonably believed to be located outside the United States differently from communications of persons located in the United States.[312] ~~(TS//STLW//SI//OC/NF)~~

A. The Protect America Act (U)

The Protect America Act of 2007, Pub. L. No. 110-55, was a temporary measure signed into law on August 5, 2007.[313] The Protect America Act's chief objective was to exclude from the requirements of FISA the interception in the United States of communications of persons located outside the United States, the category of communications referred to above as "foreign selectors." (U)

The Protect America Act amended FISA so that the interception of foreign selector communications fell outside the statute's definition of "electronic surveillance." Under the original definition of "electronic surveillance," FISA generally applied to any communication to or from a known United States person inside the United States if the communication is acquired by targeting the known United States person.[314] FISA also

---

311 The NSA also targeted under Stellar Wind a much smaller number of facilities located inside the United States (domestic selectors). ~~(TS//STLW//SI//OC/NF)~~

312 The two laws did not substantially affect the provisions of FISA relating to pen register and trap and trace surveillance or to the production of "tangible things." The government continues to collect bulk e-mail and telephone meta data under the PR/TT and Section 215 Orders described in Sections I and II of this chapter. ~~(TS//SI//NF)~~

313 The Protect America Act was set to expire 180 days after its enactment, or on February 1, 2008. However, Congress passed and on January 31, 2008, the President signed a bill to extend the Protect America Act for 15 days while further discussions on new legislation occurred. However, no agreement was reached on new legislation and the Act expired on February 16, 2008. (U)

314 The original FISA definition of "electronic surveillance" included:

(Cont'd.)

applied to the acquisition of other communications (such as communications acquired by targeting persons outside the United States) if the communication was a "wire communication" and the acquisition occurred inside the United States. (U)

The Protect America Act amended FISA by stating: "Nothing in the definition of electronic surveillance . . . shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States." The effect of this amendment was to exclude from the requirements of FISA any communication acquired by targeting a foreign selector, regardless of where the communication was intercepted or whether the communication traveled by wire. As a result, the Act eliminated the need for Judge Vinson's May 2007 foreign selectors Order, because the collection of communications targeted under that Order no longer constituted "electronic surveillance" under FISA and therefore no longer required FISA Court orders.[315] ~~(TS//SI//NF)~~

---

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(20(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. § 1801(f). (U)

315 [redacted]

(Cont'd.)

In the place of individualized FISA Court orders, the Protect America Act also inserted several provisions into the FISA statute to govern the acquisition of communications from persons "reasonably believed to be outside the United States." These provisions authorized the Attorney General and the Director of National Intelligence to acquire foreign intelligence information concerning such persons for up to one year, provided these officials certified that there are reasonable procedures in place for the government to determine that a target is reasonably believed to be outside the United States and that the acquisition of the foreign intelligence therefore is not "electronic surveillance" under the amended definition of the term.[316] The targeting procedures accompanying the certification had to be submitted to the FISA Court for approval, based on the clearly erroneous standard, within 120 days of the Protect America Act's enactment. However, the certification was not required to identify specific facilities or places at which the acquisition of foreign intelligence information would be directed.[317] (U)

In addition, the Protect America Act authorized the Attorney General and the Director of National Intelligence to direct a person (telecommunications carriers) to provide the government with "all information, facilities, and assistance necessary to accomplish the acquisition in such a manner as will protect the secrecy of the acquisition. . . ." Protect America Act, Sec. 2(e). The Protect America Act also authorized the Attorney General and the Director of National

---

[redacted] The Protect America Act addressed this issue by excluding all surveillance directed at persons reasonably believed to be outside the United States. ~~(TS//SI//NF)~~

316 The Attorney General and the Director of National Intelligence also had to certify that the acquisition involves the assistance of a communications service provider; that a "significant purpose" of the acquisition to obtain foreign intelligence information is for foreign intelligence purposes; and the minimization procedures to be used with the acquisition activity comport with 50 U.S.C. § 1801(h). Protect America Act, Sec. 2, codified in FISA at 50 U.S.C. § 1805B(a)(1)-(5). (U)

317 The Protect America Act left unchanged the procedures for acquiring foreign intelligence information by targeting foreign powers or agents of foreign power inside the United States, as well as the procedures under Executive Order 12333 Sec. 2.5 to obtain Attorney General approval before acquiring foreign intelligence information against a U.S. person outside the United States. Thus, FISA orders issued prior to the enactment of the Protect America Act, and FISA orders, including applications for renewals, sought after enactment of the Protect America Act but not pursuant to the Act's amendments (acquisition of foreign intelligence information from targets outside the United States) were still subject to FISA as it existed prior to the Protect America Act. The Protect America Act also provided, by means of an "opt-out" clause, that the government did not have to use the new procedures for new applications and could instead file applications under the provisions of FISA as it existed before the Protect America Act. See Protect America Act, Sec. 6(b). (U)

Intelligence to seek the assistance of the FISA Court to compel compliance with such directives, and implemented procedures for the telecommunications carriers to challenge the legality of any such directives.[318] (U)

The Protect America Act authorized the Attorney General and the Director of National Intelligence to issue orders without individualized FISA Court approval for up to one year targeting persons reasonably believed to be outside the United States. These orders remained in effect beyond the expiration of the Protect America Act on February 16, 2008. (U)

On August 10, 2007, the Attorney General and the Director of National Intelligence filed a certification with the FISA Court, as required under the Protect America Act, relating to surveillance of persons reasonably believed to be outside the United States likely to communicate information concerning [redacted] The certification included directives for assistance to specific telecommunications carriers. ~~(TS//SI//NF)~~

[redacted] foreign selectors under Judge Vinson's Order were "rolled over" to the new Protect America Act authority. A Deputy Assistant Attorney General in the National Security Division familiar with the transition of Stellar Wind to FISA Court authority told us that the government also began to "build new selectors" under the Protect America Act and worked toward restoring the universe of foreign selectors that were first authorized for tasking under Judge Howard's January 2007 Order when content collection under Stellar Wind initially had migrated to FISA Court authority. ~~(TS//SI//NF)~~

Although the Department viewed the Protect America Act as an adequate temporary fix to those provisions of FISA seen as outdated because of changes in telecommunications technology, Department officials continued to press Congress for more permanent modernization legislation. (U)

---

[318] The Protect America Act also stated that any person providing assistance to the government pursuant to a governmental directive would not be subject to any cause of action for providing such assistance. However, the Protect America Act did not grant retroactive legal immunity to any "person," a term defined in FISA to include "any group, entity, association, corporation, or foreign power." 50 U.S.C. § 1801(m). On August 22, 2008, the FISA Court of Review upheld as constitutional the Protect America Act provision authorizing the Director of National Intelligence and the Attorney General to direct a person to assist the government in implementing the Act. See In Re: Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, No. 08-01. (U)

B. The FISA Amendments Act of 2008 (U)

On July 11, 2008, the President signed the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISA Amendments Act). This legislation, composed of four titles, replaced the Protect America Act with similar but more comprehensive surveillance authority. The provisions of the FISA Amendments Act expire, with limited exceptions, on December 31, 2012. (U)

A chief objective of the FISA Amendments Act was to change the rules for intercepting the electronic communications of persons reasonably believed to be outside the United States when the acquisition occurs in the United States. As discussed above, the Protect America Act accomplished this by amending FISA's definition of "electronic surveillance" to exclude this activity from FISA requirements. The FISA Amendments Act took a different approach. Instead of excluding the activity from the statute's definition of "electronic surveillance," the FISA Amendments Act created a new title in FISA to govern how the government may conduct this electronic surveillance. Under this approach, the FISA Amendments Act, unlike the Protect America Act, distinguishes between the targeting of non-U.S. and U.S. persons reasonably believed to be outside the United States.[319] (U)

For non-U.S. persons, the new title created by the FISA Amendments Act provides for surveillance authority similar to the Protect America Act. Instead of requiring the government to obtain individualized orders from the FISA Court to intercept communications of non-U.S. persons reasonably believed to be outside the United States, the FISA Amendments Act authorized the government to conduct any such interceptions for a period of up to one year provided that it adopts, and the FISA Court approves, general targeting procedures designed to ensure that the new authority is not used

---

[319] The Senate Select Committee on Intelligence (SSCI) prepared a section-by-section analysis of the FISA Amendments Act of 2008 explaining the significance of the FISA Amendment Act's approach. According to the SSCI report, the goal of the Protect America Act in redefining the term "electronic surveillance" was to exclude the surveillance of persons outside the United States from the individualized order requirements of FISA. However, a consequence of the term's redefinition was to broadly exempt foreign surveillance activities both of non-U.S. and U.S. persons outside the United States. The FISA Amendments Act of 2008, instead of adopting the Protect America Act's modified definition of "electronic surveillance," explicitly stated that the targeting of non-U.S. persons outside the United States shall be conducted under the new FISA procedures, which does not require an application for a FISA order. In this way, the FISA Amendments Act accomplished the same goal as the Protect America Act without exempting the targeting of U.S. persons outside the United States from FISA's individualized order requirements. (U)

to direct surveillance at persons within the United States or at U.S. persons outside the United States.[320] (U)

In contrast, to conduct U.S.-based surveillance of U.S. persons reasonably believed to be located outside the United States, the FISA Amendments Act requires the government to obtain individualized FISA Court orders for 90-day periods based on a showing of probable cause to believe that the U.S. person is outside the United States and is a foreign power or an agent, officer, or employee of a foreign power. Such surveillance previously was governed by Executive Order 12333, and required only a certification from the Attorney General, not the FISA Court. (U)

Compared to Stellar Wind, the FISA Amendments Act provides the government broader authority to acquire in the United States, with Court supervision, the communications of non-U.S. persons reasonably believed to be located outside the United States. Under Stellar Wind, the NSA was authorized to collect communications where there was probable cause to believe the communications originated or terminated outside the United States and a party to the communications was al Qaeda or a group affiliated with al Qaeda. Under the FISA Amendments Act, the NSA is authorized to collect in the United States any communications of non-U.S. persons reasonably believed to be located outside the United States, provided a significant purpose of the acquisition pertains to foreign intelligence. [redacted]

~~(TS//STLW//SI//OC/NF)~~

---

[320] Like the Protect America Act, in addition to these targeting procedures the certification the government is required to file with the FISA Court must also contain minimization procedures and state that a significant purpose of the acquisition that will be conducted is to obtain foreign intelligence information. However, unlike the Protect America Act the FISA Amendments Act does not limit the FISA Court's review of the targeting procedures to a "clearly erroneous" standard. On August 5, 2008, the government submitted to the FISA Court a certification pursuant to the FISA Amendments Act. On September 5, 2008, the Court approved the certification and the use of the targeting and minimization procedures the government submitted. ~~(S//NF)~~

[321] On the other hand, the FISA Amendments Act does not similarly broaden the government's authority to conduct surveillance of U.S. persons reasonably believed to be located outside the United States. The Presidential Authorizations did not distinguish between U.S. and non-U.S. persons, and the NSA was authorized under Stellar Wind to intercept the communications of U.S. persons (domestic selectors) provided the communications originated or terminated outside the United States. ~~(TS//STLW//SI//OC/NF)~~

In Chapter Three, we noted that under certain circumstances technological limitations associated with the e-mail content aspect of the Stellar Wind program caused [redacted] ~~(TS//SI//NF)~~

The NSA undertook measures to identify and correct incidents [redacted] under Stellar Wind, and the government described the issue to the FISA Court in the December 2006 application that sought to bring Stellar Wind's content collection under FISA authority. [redacted] ~~(TS//SI//NF)~~

[redacted]

V. OIG Analysis (U)

As discussed in this chapter, the government's effort to transition Stellar Wind from presidential authority to FISA, which began in March 2004, eventually resulted in all three baskets of collection being authorized by FISA. While the legal theories supporting this transition were aggressive, we believe that the Department could have and should have pursued transition to FISA as a viable legal alternative earlier than it did, rather than operate aspects of the Stellar Wind program solely under presidential authority for several years. ~~(TS//STLW//SI//OC/NF)~~

In Chapters Three and Four we discussed John Yoo's 2001 and 2002 memoranda concerning the legality of Stellar Wind and his contention that FISA represented an unconstitutional infringement on the President's Commander-in-Chief authority under Article II of the Constitution to conduct electronic surveillance during wartime. We recognize that Yoo's analysis was to some extent a response to the extraordinary circumstances that confronted the federal government immediately after the September 11 terrorist attacks and its effort to take emergency steps to thwart what many officials believed was an imminent second wave of attacks. Yet, even if one agrees with Yoo's Article II analysis and supports the decision to enhance outside the judicial or legislative process the NSA's signals intelligence collection capabilities, we believe there are strong countervailing considerations that favored attempting to transition the program to FISA, especially as Stellar Wind became less a temporary response to the September 11 attacks and more a permanent surveillance tool. ~~(TS//STLW//SI//OC/NF)~~

Chief among these considerations was the Stellar Wind program's substantial effect on privacy interests of U.S. persons. Under Stellar Wind, the government engaged in an unprecedented collection of information concerning U.S. persons. The President authorized the NSA to intercept, without judicial approval or oversight, the content of international communications involving many U.S. persons and the NSA collected large amounts of non-content data about U.S. persons' domestic and international telephone calls and to a lesser extent e-mail communications for possible analysis consistent with the extant Presidential Authorization. We believe the FISA Court, as an Article III court and the judicial authority charged by statute to oversee U.S.-based electronic surveillance and other collection activities affecting U.S. persons for foreign intelligence purposes, was the appropriate entity to monitor and approve such broad acquisitions

of U.S.-person information conducted under Stellar Wind.[322] ~~(TS//STLW//SI//OC/NF)~~

Second, as several Justice Department and NSA officials commented, the FISA statute offered a "firmer footing" for the NSA's collection activities under Stellar Wind. As discussed in Chapter Three and Four, the aggressive assertion of Article II authority on which Stellar Wind was based largely reflected the legal reasoning of a single Justice Department attorney working alone, without adequate review or scrutiny of his analysis. As we also concluded, this led to a flawed legal analysis on which the program rested for several years. This approach also led to a contentious dispute between Department and White House officials in 2004 involving renewal of aspects of the program. By contrast, the FISA statute provided an alternative basis for Stellar Wind-like collection activities that we believe should have been considered, and pursued, much earlier by the Administration. ~~(TS//STLW//SI//OC/NF)~~

In this regard, the White House's strict control over the Justice Department's access to the program lessened the opportunity for lawyers with relevant expertise to advise the Administration on the viability of working within the FISA statute to achieve the same operational objectives as the Stellar Wind program. Moreover, as the limited number of Department read-ins persisted, meaningful consideration of FISA as an alternative to presidential authority for the program was limited.[323] ~~(TS//STLW//SI//OC/NF)~~

---

[322] For instance, under Stellar Wind the meta data querying standards did not include restrictions on acquiring data that may have been based solely on the exercise of First Amendment rights. When these activities were placed under the FISA Court's supervision, the Court required that this intelligence-gathering activity adhere to the FISA standard that an e-mail address or telephone number cannot be targeted for acquisition based solely on activities protected by the First Amendment. ~~(TS//STLW//SI//OC/NF)~~

[323] [redacted]

We also found there were operational benefits to transitioning Stellar Wind to FISA. The PR/TT and Section 215 Orders to collect e-mail and telephone meta data that were eventually obtained from the FISA Court allowed the government to compel [redacted] the telecommunications carriers. [redacted] (~~TS//STLW//SI//OC/NF~~)

The transition of Stellar Wind to FISA authority, together with the passage of the Protect America Act, allowed the NSA to begin the process to close, or "de-compartment," the Stellar Wind program. This change, which was not completed until mid-2008, has allowed agents in FBI field offices greater access to information about the telephone numbers and e-mail addresses being provided as leads. As described in Chapter Three, the principal complaint of agents who were assigned [redacted] and [redacted] leads was the lack of detail provided about the nature of the international contacts and the foreign entity allegedly involved with terrorism that was one of the communicants. These details often were not provided because of the highly classified and compartmented nature of the Stellar Wind program. Now that such information is gathered under FISA authority and not compartmented as it was under Stellar Wind, it is classified at a level that allows agents in FBI field offices to gain access to additional details upon request.[324] ~~(TS//STLW//SI//OC/NF)~~

We recognize that Stellar Wind's transition to FISA resulted in the imposition of new responsibilities and conditions on the exercise of these unprecedented collection authorities. In the PR/TT and Section 215 Orders, the FISA Court imposed significant oversight measures that were not required under Stellar Wind. To be sure, the government, particularly the NSA, must devote substantial resources to ensure compliance with these oversight measures. Yet, we believe that such requirements are appropriate, given the massive amounts of data collected and the potential impact on the privacy interests of U.S. persons. ~~(TS//STLW//SI//OC/NF)~~

We also recognize that the transition of content collection from presidential authority to statutory authority under FISA resulted in significant diminution in authorized surveillance activity of the content of communications. We described in this chapter how first under Judge Howard's Order, and then more significantly under Judge Vinson's revised

---

[324] Chapter Six of this report discusses FBI agents' improved access to program-derived information under FISA after the Stellar Wind program was closed. ~~(TS//SI//NF)~~

Order, the NSA placed increasingly fewer foreign selectors under FISA coverage as compared to Stellar Wind. The NSA was tasking [redacted] foreign selectors under Stellar Wind at the time of the first content application in December 2006, but placed [redacted] foreign selectors under surveillance coverage under Judge Vinson's May 2007 Order. National Security Division officials told us that they successfully added approximately [redacted] foreign selectors under the terms of the Court's Order. ~~(TS//STLW//SI//OC/NF)~~

However, we believe that such broad surveillance and collection activities conducted in the United States, particularly for a significant period of time, should be conducted pursuant to statute and judicial oversight, even though this resulted in a diminution of foreign selectors due to resource issues. We also believe that placing the activities under Court supervision provides an important measure of accountability for the government's conduct that is less assured when the activities are both authorized and supervised by the Executive Branch alone.[325] ~~(TS//STLW//SI//OC/NF)~~

In sum, we concluded there were compelling reasons to pursue beginning the process of transitioning the collection activities of Stellar Wind to FISA authority earlier than [redacted] 2004. These included the program's large collection of information about U.S. persons, which warranted judicial oversight; the instability of the legal reasoning on which the program rested for several years; and the substantial restrictions placed on FBI agents' access to and use of program-derived information due to Stellar Wind's highly classified status. We acknowledge that transitioning Stellar Wind's collection activities to FISA would have been an enormously complex and time-consuming effort that rested upon novel interpretations and uses of FISA that not all FISA Court judges would authorize. Nevertheless, the events described in this chapter demonstrate that a full transition to FISA authority was achievable and, and in our judgment, should have been pursued earlier. ~~(TS//STLW//SI//OC/NF)~~

---

[325] Even Judge Vinson's decision regarding the foreign selectors content application, [redacted] was not without benefit. Judge Vinson's decision reflected what some intelligence officials considered limitations in the FISA statute as it applied to the acquisition of communications in the United States of persons located outside the United States, especially non-U.S. persons. In this way, transitioning Stellar Wind's content collection to FISA helped the government make its case to Congress in concrete, non-hypothetical terms for modernization legislation amending the statute. ~~(TS//STLW//SI//OC/NF)~~

CHAPTER SIX
[redacted] (~~S//NF~~)

The preceding chapters examined the evolution of the Stellar Wind program and its transition from Presidential Authorization to FISA authority. In this chapter, we examine more closely the FBI's involvement in Stellar Wind and the impact the program had on FBI counterterrorism efforts. ~~(TS//STLW//SI//OC/NF)~~

[redacted] is the codename for the project, classified at the Secret level, that the FBI initiated in September 2002 to disseminate Stellar Wind information to FBI field offices in a manner that did not disclose the source of the information or the means by which it was acquired. The FBI originally opened [redacted] as an administrative file to serve as the repository for all communications FBI Headquarters disseminated to FBI field offices relating to Stellar Wind information, as well as all communications FBI Headquarters received from field offices reporting the results of any investigation conducted in response to the "tipped" information originating from Stellar Wind. In November 2006, the FBI opened an investigative file under the name [redacted][326] ~~(TS//STLW//SI//OC/NF)~~

Section I of his chapter summarizes how the FBI used [redacted] to disseminate Stellar Wind information to FBI field offices. Section II describes the FBI's decision in mid-2003 to make its headquarters-based Communications Analysis Unit (CAU), instead of FBI field offices, responsible for issuing National Security Letters (NSL) to obtain subscriber information for telephone numbers (basket 2 of Stellar Wind) disseminated under [redacted].[327] Section III discusses the role the FBI played, beginning in approximately March 2004, in the process to "scrub" international terrorism FISA applications for Stellar Wind information. ~~(TS//STLW//SI//OC/NF)~~

Section IV of this chapter examines the impact of the information obtained from Stellar Wind on FBI counterterrorism efforts. It first provides statistics concerning the number of tippers the NSA derived from Stellar Wind information – telephony, e-mail, and content – disseminated to FBI

---

[326] As discussed in Chapter Three, [redacted] was preceded by the [redacted] which the FBI created in October 2001 to receive and disseminate Stellar Wind-derived information. ~~(TS//STLW//SI//OC/NF)~~

[327] The CAU is the successor to the Telephone Analysis Unit (TAU), which the FBI created after the September 11 terrorist attacks to analyze telephone communications. The CAU assumed TAU's responsibilities in late 2002. ~~(S//NF)~~

field offices through the [redacted] process. Next, it describes how FBI field offices generally investigated [redacted] tippers and the typical results of the investigations. The section then summarizes two statistical surveys of meta data tippers the FBI conducted in 2006 to assess the value of Stellar Wind to FBI operations, and describes observations about the program's contribution and value provided by FBI officials and employees in OIG interviews and contained in documents the OIG obtained during the course of this review. In addition, the section examines five FBI international terrorism investigations commonly cited as examples of Stellar Wind's contribution to counterterrorism efforts in the United States.[328] ~~(TS//STLW//SI//OC/NF)~~

Lastly, Section V of this chapter contains the OIG's analysis of [redacted] impact on FBI operations. ~~(S//NF)~~

I. [redacted] Process ~~(S//NF)~~

The [redacted] process was managed by a group of FBI employees from CAU, designated as "Team 10," who in February 2003 were assigned full-time to the NSA to work on the Stellar Wind program.[329] Team 10 was described to us as a "conduit" and a "curtain" between Stellar Wind and the FBI, in that Team 10's chief responsibility was to disseminate Stellar Wind-derived information to FBI field offices for investigation without disclosing that the NSA was the source of the information or how the NSA acquired the information. ~~(TS//STLW//SI//OC/NF)~~

Team 10 initially was staffed with two FBI special agents (one of whom served as supervisor) and two analysts. The CAU subsequently replaced one agent position with a third analyst and later added a fourth analyst. At the NSA, Team 10 was co-located in a large open space with dozens of NSA and other Intelligence Community personnel assigned to the Stellar Wind program. Each team member was provided a computer with direct access to NSA information associated with Stellar Wind. The NSA told the OIG that Team 10 members worked at the NSA under the authority of the NSA Director and as such were required to adhere to NSA minimization rules and attend the same training as NSA employees. Team 10 members also were provided access to Stellar Wind-related systems and

---

[328] As noted above, our report examines the FBI's role in the Stellar Wind program and does not review the use of the program by other agencies, such as the CIA. ~~(S//NF)~~

[329] The CAU is organized into ten teams, nine of which are responsible for providing communications analysis support to specific field offices and FBI Legal Attaches (Legat). According to an FBI organizational chart, Team 10 supports "Off-site Intelligence Community Special Projects." Team 10 was exclusively responsible for managing [redacted] ~~(S//NF)~~

databases, and had access from their computers to FBI systems such the Automated Case Support (ACS) system and [redacted] ~~(TS//STLW//SI//OC/NF)~~

The process under [redacted] to disseminate Stellar Wind information was similar to the process the FBI established under the [redacted] described in Chapter Three. In short, the NSA provided Top Secret, compartmented Stellar Wind reports to Team 10, which in turn converted the information into Secret, non-compartmented [redacted] electronic communications (EC) and disseminated the communications, referred to as [redacted] "tippers," to FBI field offices for appropriate action.[330] The [redacted] process was applied, with some differences, to each of Stellar Wind's three "baskets" of information. The vast majority of Stellar Wind reports involved the NSA's analysis of telephony meta data – that is, basic information such as date, time, and duration, about contacts between foreign and domestic telephone numbers for which the NSA determined there was a reasonable articulable suspicion to believe were related to al Qaeda or an affiliated group.[331] ~~(TS//STLW//SI//OC/NF)~~

Each [redacted] EC included a paragraph that summarized the [redacted] project and explained that the CAU could not disclose the source of the information contained in the EC, but that the information came from a "sensitive and highly reliable" source. Each EC also included a paragraph advising the field offices that the information provided by the [redacted] source could be used for "lead purposes only" and could not be "incorporated into any affidavit, court proceeding, FISA application or

330 [redacted]

331 [redacted]

unclassified investigative file." In addition, each [redacted] EC assigned a "lead" that instructed the field office what investigative action, if any, should be taken regarding the information provided. We further describe [redacted] leads and FBI field offices' handling of them in Section IV of this chapter. ~~(TS//STLW//SI//OC/NF)~~

Before Team 10 disseminated Stellar Wind-derived information to field offices, an analyst queried FBI databases for relevant information about the telephone number, e-mail address, or individual (in the case of a content report) identified in the Stellar Wind report. These queries often identified, for example, subscriber information the FBI previously obtained for Stellar Wind telephone numbers as part of a prior FBI investigation, or active counterterrorism investigations in which the subscriber to a Stellar Wind-targeted number was the subject or in which the number, and sometimes the subscriber, were referenced. Team 10 analysts also checked public and commercial databases, most commonly in connection with e-mail addresses. These checks sometimes identified the specific [redacted] and any domain names the user of an e-mail address had registered. [redacted] Any such information Team 10 located about a Stellar Wind-derived telephone number or e-mail address was included in the [redacted] EC as a "CAU Comment" or an "Analyst Comment" to differentiate the FBI information from the information provided by the Stellar Wind source.[332] ~~(TS//STLW//SI//OC/NF)~~

Over time, Team 10 began to do more than receive and disseminate program-derived information. For example, Team 10 occasionally submitted telephone numbers to the NSA for possible querying against the database containing the bulk telephony meta data collected under Stellar Wind.[333]

---

[332] In this respect, Team 10 handled Stellar Wind content reports differently from meta data reports. Team 10 analysts typically did not perform additional analytical work on the information provided in Stellar Wind content reports other than to identify any FBI cases to which the information was relevant. For example, a content report might summarize intercepted communications indicating that an acquaintance of the subject of an FBI investigation is traveling to or from the United States. The connection between this Stellar Wind information and the relevant FBI investigation would be reported in the [redacted] EC. ~~(TS//STLW//SI//OC/NF)~~

[333] As described in previous chapters, the purpose of the bulk collection of meta data under Stellar Wind was to allow the NSA to use analytical tools such as contact chaining [redacted] to identify known and unknown individuals associated with al Qaeda or an al Qaeda affiliate. The technique involves querying the telephony or e-mail database with a number or address for which an analyst had a "reasonable articulable suspicion" to believe was used by persons involved in al Qaeda or an al Qaeda affiliate, and then examining any contacts with that number or address. ~~(TS//STLW//SI//OC/NF)~~

The telephone numbers Team 10 provided typically were obtained from the FBI's domestic and international counterterrorism operations, such as a number identified during a phone conversation monitored under FISA or a number found in the address book of a subject arrested abroad. The NSA conducted independent analysis to determine whether telephone numbers (or e-mail addresses) provided by Team 10 met the querying standard established by the Presidential Authorizations that governed Stellar Wind (that is, a reasonable articulable suspicion to believe that communications from the telephone number relate to al Qaeda or an affiliated group).[334] ~~(TS//STLW//SI//OC/NF)~~

Team 10 also contributed to the NSA's drafting process for Stellar Wind reports. Telephone numbers and e-mail addresses identified through queries of the databases that contained the bulk telephony and e-mail meta data were reviewed by NSA analysts to determine whether the contacts should be reported to the FBI in a Stellar Wind report. Team 10 participated in this process by reviewing draft reports and providing any information from FBI databases that might be relevant to this determination.[335] ~~(TS//STLW//SI//OC/NF)~~

We were told that one of the benefits of Team 10's presence at the NSA and its involvement in the Stellar Wind report drafting process was an improvement in the quality of the information disseminated to FBI field offices. For example, the FBI Supervisory Special Agent (SSA) who supervised Team 10 from April 2005 to July 2006 told the OIG that he tried to reduce the NSA's reporting of telephone numbers that were several hops removed from the telephone number linked to al Qaeda or an affiliated terrorist group. He said that he wanted Team 10 to disseminate "solid numbers with value," not numbers with questionable value such as "high volume numbers" (public telephones, for example) and [redacted] The FBI SSA said that the NSA expressed the concern

---

[334] Team 10 analysts submitted such telephone numbers to the NSA electronically through "Requests for Information," or RFIs, which is the formal process by which the FBI and other agencies provide leads and request information from the Stellar Wind database. FBI records indicate that from April 2002 to January 2006 the FBI directed [redacted] to NSA analysts for possible analysis under Stellar Wind. The records do not indicate the disposition of each RFI. ~~(TS//STLW//SI//OC/NF)~~

[335] The NSA developed formal "checklists" to guide the Stellar Wind report drafting process for telephony and e-mail tippers. The checklists include over 30 steps that NSA analysts were required to complete, and a supervisor had to approve, before a report could be distributed to the FBI or any other Stellar Wind customers (the CIA and National Counterterrorism Center). A significant feature of the checklist from the FBI's perspective was the requirement that NSA analysts check any telephone numbers and e-mail addresses in a draft report with the FBI and "make best effort to include FBI . . . data in [the] tipper." ~~(TS//STLW//SI//OC/NF)~~

that it could not foresee whether any particular contact, although remote, might prevent the next terrorist attack, and did not want to find itself in the position of defending its decision not to pass that number to the FBI. However, he said the NSA took several steps to improve the quality of information such as [redacted] for the domestic contacts that were reported and including analytical judgments about the contacts.[336] ~~(TS//STLW//SI//OC/NF)~~

As discussed in Chapter Five, the government transitioned Stellar Wind's bulk e-mail meta data collection (basket 3) to FISA authority in July 2004 with the Pen Register/Trap and Trace Order, bulk telephony meta data collection (basket 2) in May 2006 with the Section 215 Business Records Order, and content collection (basket 1) in January 2007 when the FISA Court granted the government's domestic and foreign selectors applications. ~~(TS//STLW//SI//OC/NF)~~

However, after the transition was completed the NSA continued to produce reports within the Stellar Wind compartment to the FBI and other program customers, even though the information contained in the reports was derived from the FISA-authorized collection activities. Consequently, the FBI continued to disseminate the information under the [redacted] process. The current Team 10 supervisor told us that this decision, reached after consultation with the FBI's Office of the General Counsel (OGC), was made to adhere to the FISA Court's continuing requirement that international terrorism FISA applications be scrubbed for Stellar Wind information (the procedure for which is described in Section III of this chapter). ~~(TS//STLW//SI//OC/NF)~~

The NSA received permission to begin the process to close, or "de-compartment," the Stellar Wind program after the Protect America Act was passed in August 2007. In mid-2008, the NSA officially closed the program and discontinued issuing "Stellar Wind" reports. In November 2008, the FBI initiated a new investigative file, [redacted] to disseminate the NSA's FISA-derived information.[337] The Team 10 supervisor

---

[336] The NSA told us that one of the difficulties it faced with the Stellar Wind program was that the NSA was serving two customers – the FBI and the CIA – but had just one set of reporting guidelines. This was so because the NSA traditionally does not provide single-agency reporting except in narrowly defined circumstances. [redacted] ~~(S//NF)~~

[337] According to the FBI memorandum explaining the predication for opening the file, the focus of [redacted] investigation is on known and unknown operatives of [redacted] The memorandum stated that as of August 2008 the FBI had [redacted] open national security investigations related to [redacted] of individuals believed to be associated with [redacted] (Cont'd.)

told us that the dissemination process and the FBI's coordination with the NSA under [redacted] is similar to what occurred under [redacted] However, one notable difference is that the NSA's FISA-derived reports, while classified at the Top Secret/Sensitive Compartmented Information (TS/SCI) level, are not subject to the highly restrictive Stellar Wind compartment designation, which is significant from an operational standpoint. [redacted] ECs, like [redacted] ECs, can only include information classified Secret or lower because the FBI's primary computer network for disseminating communications cannot be used for Top Secret information. Unlike under [redacted] agents in field offices can now request access to additional information about [redacted] leads because agents have the appropriate clearances. As discussed in Chapter Three and addressed below, the chief criticism of [redacted] leads was the lack of detailed information that could be provided to field agents about tippers because of the highly compartmented nature of Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

II. FBI's Decision to Issue National Security Letters under [redacted] to Obtain Telephone Subscriber Information ~~(S//NF)~~

From August 2003 to November 2006, as part of the [redacted] process the Communications Analysis Unit (CAU) assumed responsibility from the field offices for requesting National Security Letters (NSL) to obtain subscriber information for [redacted] telephone number tippers.[338] The NSLs were authorized by the FBI's OGC and issued pursuant to the [redacted] project. As discussed below, however, this practice was contrary to applicable FBI investigative guidelines because [redacted] was opened as a non-investigative file and therefore under FBI policy should not have been used as the basis for issuing NSLs. ~~(S//NF)~~

The FBI uses NSLs to obtain information from third parties such as telephone companies, financial institutions, Internet service providers, and consumer credit agencies. NSLs, authorized by five specific provisions contained in four federal statutes, direct third parties to provide customer account information and transactional records such as telephone toll billing

[redacted] of individuals believed to be associated with [redacted] and [redacted] of [redacted] ~~(S//NF)~~

[338] Field offices remained responsible for issuing NSLs in connection with e-mail address tippers, which was likely attributable to the comparatively low volume of e-mail tippers and the ability of field offices to handle them expeditiously. ~~(S//NF)~~

records.[339] The OIG issued two reviews in 2007 and 2008 examining the FBI's use of NSLs.[340] (U)

Justice Department investigative guidelines issued by the Attorney General govern the circumstances under which the FBI may use NSLs. The Attorney General guidelines in effect during the Stellar Wind program authorized the FBI to issue NSLs relevant to and in the course of an authorized national security investigation.[341] Further, FBI internal policy distinguishes between "investigative files" and non-investigative "administrative files" (commonly referred to as "control files"). This distinction is not a mere technicality. Investigative files, in the national security context, are opened based on evidence that a person, group, or organization is involved in international terrorism. From October 2003 to September 2008, the Attorney General Guidelines required the FBI to provide summary reports to the Justice Department at the end of each year

---

[339] The four federal statutes are the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422; the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709; the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.; and the National Security Act, 50 U.S.C. § 436(a)(1) (2000). NSLs issued under [redacted] relied on the ECPA statute, which provides that the FBI may obtain subscriber information from a communications service provider if the FBI certifies that the information sought is

> relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.

18 U.S.C. § 2709(b)(2) (2000 & Supp. IV 2005). The statute also permits access to "toll billing records" or "electronic communication transactional records," 18 U.S.C. § 2709(a), but requires a warrant for access to the content of telephone communications. See 18 U.S.C. § 2511 (Wiretap Act) and 3121 (Pen Register Act); see also 18 U.S.C. § 2702(b)(8). (U)

[340] The OIG's first report on NSLs, issued in March 2007, was entitled, *A Review of the Federal Bureau of Investigation's Use of National Security Letters.* The OIG's second report, issued in March 2008, was entitled, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006.* (U)

[341] From March 8, 1999, through October 31, 2003, national security investigations were governed by the Attorney General's Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCI Guidelines). The FCI Guidelines were replaced, effective October 31, 2003, with the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines). (U)

The evidentiary standard for initiating an investigation is the same under both sets of guidelines. To open a full investigation, the FBI is required to demonstrate [redacted] A preliminary investigation (or "inquiry," under the FCI guidelines) requires only a showing of [redacted] of such involvement. See NSI Guidelines, Section II.C. (October 31, 2003); FCI Guidelines, Section III.B. (March 8, 1999). ~~(S//NF)~~

a full national security investigation continues. These requirements helped ensure that there was sufficient, documented predication for investigative activities FBI agents sought to conduct, such as requesting NSLs. ~~(S//NF)~~

Control files, in contrast, are "separate files established for the purpose of administering specific phases of an investigative matter or program." The files do not require any predication and remain open indefinitely without any reporting requirements for national security investigations. For example, the September 2002 EC requesting that a control file [redacted] be opened for Stellar Wind information stated that "a dedicated control file for this project will better serve the specific needs of the special project and will add an additional layer of security for the source." The file has remained open since September 2002 without any official documentation of need or justification. (As discussed below, in November 2006 the FBI opened an [redacted] investigative file; however, the [redacted] control file was not closed at that time.) ~~(TS//STLW//SI//OC/NF)~~

The FBI's National Foreign Intelligence Program (NFIP) Manual states that [redacted].[342] Thus, in accordance with the NFIP Manual, it was improper for the FBI to issue NSLs from control files during the Stellar Wind program. ~~(S//NF)~~

The OIG's March 2007 NSL report identified the [redacted] project as one of two circumstances where the FBI was using control files rather than investigative files to issue NSLs. The OIG report concluded that this use was contrary to FBI policy. However, our report also found that the CAU officials involved in the decision to issue NSLs from the [redacted] control file concluded in good faith that the FBI had sufficient predication either to connect the [redacted] NSLs with existing preliminary or full investigations of al Qaeda and affiliated groups or to open new preliminary or full investigations in compliance with Justice Department investigative guidelines. ~~(S//NF)~~

[redacted]

As part of our review of the FBI's participation in Stellar Wind, we sought additional explanation for the use of NSLs under [redacted] We were told the purpose of having the CAU instead of the field offices obtain approval for the issuance of such NSLs was to make the telephony tippers more "actionable" by ensuring that field offices at a minimum knew the subscribers for the numbers. As described in Chapter Three, the members of the [redacted] (the predecessor to [redacted]) had received complaints from agents in FBI field offices that [redacted] leads lacked direction about how to make investigative use of the telephone numbers and did not provide sufficient information to open national security investigations. This was problematic because leads disseminated under the [redacted] and for a time under [redacted] instructed field offices to obtain subscriber information for tipped telephone numbers. Thus, if agents could not locate the information in FBI or commercial databases, they faced a dilemma about how to proceed in the absence of what they viewed as sufficient predication. ~~(TS//STLW//SI//OC/NF)~~

The CAU's first Unit Chief (who served in an Acting capacity) discussed the problem in an EC distributed in January 2003 that addressed the [redacted] project. The EC stated,

> Depending on the nature of the information provided [in an [redacted] lead], field offices may determine this intelligence could be used to predicate either a criminal investigation or an intelligence investigation of someone in their territory. Some of the [redacted] leads may contain a request for a field office to confirm a subscriber in their territory, if possible, in addition to providing intelligence. The identification of some subscribers might actually require a National Security Letter (NSL) or a Grand Jury subpoena; however, the [redacted] control file would not be the appropriate legal authority for these requests. ~~(S//NF)~~

The Acting Unit Chief's supervision of the CAU ended in February 2003. In March 2003, another FBI Supervisory Special Agent (SSA) was appointed as the CAU's first permanent Unit Chief. He told us that when he joined the CAU he was aware that field offices sometimes did not obtain subscriber information on tippers because some agents did not believe [redacted] ECs provided sufficient information to open a national security investigation. The Unit Chief disagreed, based in part on his insider knowledge about how Stellar Wind operated. He said that he believed the

[redacted] tippers contained sufficient information to open preliminary investigations and issue NSLs.[343] ~~(TS//STLW//SI//OC/NF)~~

The Unit Chief wanted field offices at a minimum to know the identity of subscribers of tipped telephone numbers. He also said it was important to ascertain the correct identities of the subscribers at the time the tipped calls were placed. The Unit Chief stated that if the field office did not issue an NSL for subscriber information promptly, or if the field office relied only on publicly available information, the passage of time could cause the user of the phone to be misidentified. In addition, the Unit Chief said that even if a tipper did not result in any investigative value at the time of the tip, it nevertheless was important to identify the subscriber in the event the tipper became relevant in the future or to another investigation. For all of these reasons, the Unit Chief said he took steps to make the CAU, instead of the FBI field offices, responsible for issuing NSLs for telephone number tippers under the Stellar Wind program.[344] ~~(TS//STLW//SI//OC/NF)~~

In approximately July 2003, a CAU analyst was read into the Stellar Wind program to process [redacted] NSLs. The analyst told us she questioned the Unit Chief and the Team 10 supervisor about whether it was permissible to issue NSLs out of a control file. The Unit Chief told us that he was not aware at this time that a control file such as [redacted] could not be used to issue NSLs. ~~(TS//STLW//SI//OC/NF)~~

The analyst volunteered to approach FBI OGC and met with Marion "Spike" Bowman of the OGC's National Security Law Unit to discuss this concern. She said she told Bowman that the CAU wanted to know if it could issue NSLs under [redacted] in view of its status as a control file. She said she told Bowman that the NSLs would seek subscriber information only and that field offices would be responsible for seeking related toll billing records if warranted by additional investigation. ~~(TS//STLW//SI//OC/NF)~~

According to the analyst, Bowman said that it would be permissible to issue NSLs out of the [redacted] file as long as only subscriber information was sought. The analyst said she could not recall whether Bowman affirmatively stated that issuing NSLs from a control file would be

---

[343] On January 16, 2003, 2 months before the FBI SSA was appointed Unit Chief of the CAU, Attorney General Ashcroft authorized the FBI to issue NSLs during preliminary investigations. Prior to this time, the FCI guidelines authorized the FBI to issue NSLs only as part of a "full investigation." ~~(S//NF)~~

[344] The Unit Chief told us that he did not believe it was critical at the preliminary stage to also obtain telephone subscribers' calling records, or "toll records," identifying all outgoing and incoming calls. ~~(TS//STLW//SI//OC/NF)~~

permissible or whether he merely agreed that it would be permissible under the conditions the analyst presented.[345] ~~(TS//STLW//SI//OC/NF)~~

Shortly after the meeting, the CAU implemented procedures for requesting that OGC issue NSLs to obtain subscriber information for each [redacted] telephone number tipper disseminated to field offices that the FBI was not already aware of or for which it did not have subscriber information. Under these procedures, the CAU analyst received a copy of each [redacted] EC with telephone number tippers as they were issued by Team 10 and drafted a separate approval EC to the NSLB that repeated this information and requested that the NSLB issue NSLs for the numbers listed. NSLB attorneys were responsible for determining whether the NSL requests were "relevant to an authorized investigation," as required by statute. If the attorneys determined that they were, NSLs were drafted and signed by the Deputy General Counsel for NSLB and forwarded to the CAU for service on the appropriate communications service providers. The providers returned the responsive records to the CAU, which in turn disseminated the information to the appropriate FBI field offices. From August 2003 to November 2006, the CAU issued over 500 NSLs under [redacted] ~~(TS//STLW//SI//OC/NF)~~

We interviewed FBI Deputy General Counsel Julie Thomas about NSL issuance practices under [redacted] Thomas was read into Stellar Wind shortly after joining the NSLB in October 2004. She was responsible for reviewing and authorizing [redacted] NSLs requested by the CAU. Thomas said she was familiar with the operational reasons the CAU began issuing NSLs under [redacted] but stated that it was not until the OIG was conducting its first review of the FBI's use of NSLs in 2006 that she learned [redacted] was a control file and the significance of this status as it related to issuing NSLs. Thomas said that the CAU's requests to NSLB to authorize NSLs under [redacted] always identified the specific file number associated with the project and indicated that the CAU had initiated a preliminary inquiry in connection with the NSL request. Thus, in Thomas's view, the NSL being requested was "relevant to" an authorized investigation, as

---

[345] FBI General Counsel Valerie Caproni told the OIG that she believes Bowman based his guidance to the CAU on the understanding that the NSA, by reporting a tipper to the FBI, already had established a reasonable articulable suspicion that the foreign end of the contact was related to al Qaeda or an affiliated group. Caproni said that in view of the hundreds of al Qaeda investigations the FBI was conducting, Bowman likely concluded it was permissible to issue NSLs under [redacted] for the subscriber information of tippers even if at the time there was not a specific investigation to which each NSL could be connected. The Team 10 supervisor at this time told the OIG that he recalled the decision to issue NSLs from [redacted] was based on [redacted] close relationship to the FBI's ongoing investigations of al Qaeda and affiliated groups. ~~(TS//STLW//SI//OC/NF)~~

required by statute and Justice Department investigative guidelines.[346] ~~(TS//STLW//SI//OC/NF)~~

However, Thomas said she did not believe the [redacted] NSLs were improper even though they were issued from a control file. Thomas stated that the NSLs in fact were relevant to authorized international terrorism investigations in that the FBI was conducting hundreds of investigations of al Qaeda and its affiliates at the time the NSLs issued. Thomas told the OIG that, notwithstanding this position, in November 2006 the FBI converted [redacted] to an "umbrella investigative file" to reflect the program's relationship to international terrorism investigations. ~~(TS//SI//NF)~~

The OIG reviewed the communication from the CAU opening this investigative file. It stated that a member of the U.S. Intelligence Community [the NSA] reported to the FBI that al Qaeda members and associates are using telecommunications systems to facilitate their terrorist activities, that the FBI has independently determined that this is occurring, and that "inasmuch that Al-Qa'ida is a multi-faceted and international terrorism organization, the FBI has determined it is appropriate to open a full field investigative [sic]." The communication stated that the CAU was using information obtained from the member of the U.S. Intelligence Community to issue NSLs and that the results are disseminated to the appropriate FBI field offices. The communication also advised that all investigative leads associated with the investigation would be titled [redacted] to protect the source of the information and the methods used to obtain the information. ~~(TS//STLW//SI//OC/NF)~~

The FBI currently is taking a similar approach to NSLs under the [redacted] A field office (instead of the CAU) is authorized to issue an NSL under the [redacted] investigative file, even if the field office does not open its own investigation and the tipped domestic telephone number or e-mail address is not relevant to another open investigation. However, NSLs issued under [redacted] can request subscriber information only and may not request transactional records, as was done under [redacted] ~~(TS//SI//NF)~~

The FBI's decision to restrict [redacted] NSLs in this way was not required by law, but was an operational decision. As discussed below, FBI

---

[346] The [redacted] file number is [redacted] Thomas told us that she did not realize that the "C" designation stood for "Control File." In addition, in the approval ECs reviewed by the OIG that sought the issuance of NSLs, the CAU stated, among other things, that the [redacted] source" reported telephonic contact between possible al Qaeda or other international terrorism entities and numbers in the United States and that "a preliminary CAU inquiry was conducted for the US telephone numbers reported by this source." ~~(TS//STLW//SI//OC/NF)~~

field offices addressed most [redacted] tippers by conducting "threat assessments" to determine whether the tipper had a nexus to terrorism and warranted the field office initiating a preliminary or full investigation. The subscriber information for a tipper is sufficient for purposes of completing a threat assessment. The same is true for [redacted] tippers, and the current Team 10 supervisor told us that it would not be a "good business" practice to collect transactional records on a U.S. person unless a threat assessment justified the field office initiating its own preliminary or full investigation of the individual. ~~(TS//SI//NF)~~

We believe the FBI should have opened an [redacted] investigative file in July 2003 and used it to issue NSLs related to Stellar Wind information. The Justice Department investigative guidelines in effect at that time authorized the FBI to open full investigations of groups for which there were specific and articulable facts to believe were involved in international terrorism, such as al Qaeda. However, the FBI decided to issue Stellar Wind NSLs from an existing control file, which was contrary to FBI internal policy. ~~(TS//STLW//SI//OC/NF)~~

We did not find evidence that officials from the CAU and OGC involved in the decision to use an existing control file to issue NSLs related to Stellar Wind information deliberately tried to circumvent FBI guidelines. The July 2003 rationale for issuing the NSLs out of the control file – the close relationship between the Stellar Wind program and the FBI's ongoing investigations of al Qaeda and affiliated groups – essentially was the reasoning used in November 2006 to open the [redacted] investigative file and in November 2008 to open the [redacted] investigative file. As we found in our March 2007 report concerning the FBI's use of NSLs, the CAU and OGC officials involved in the decision to issue NSLs from the [redacted] control file concluded in good faith that the FBI had sufficient predication either to connect the [redacted] NSLs with existing preliminary or full investigations of al Qaeda and affiliated groups or to open new preliminary or full investigations in compliance with Justice Department investigative guidelines. Nevertheless, the decision violated FBI internal policy. ~~(TS//STLW//SI//OC/NF)~~

III. [redacted] and Scrubbing Process ~~(TS//SI//NF)~~

As discussed in Chapter Three, the Department implemented a process imposed by the FISA Court to "scrub" FISA applications to account for Stellar Wind-derived information. The objectives of the initial scrubbing process were to determine whether any NSA information contained in international terrorism FISA applications was derived from Stellar Wind and whether any of the facilities (telephone numbers or e-mail addresses) targeted by international terrorism FISA applications were also targeted for

Stellar Wind collection (commonly referred to as dual coverage). ~~(TS//STLW//SI//OC/NF)~~

The scrubbing process was coordinated by the Justice Department and NSA, beginning in February 2002 after Judge Lamberth was read into Stellar Wind. In May 2002, Judge Kollar-Kotelly succeeded Judge Lamberth as Presiding Judge of the FISA Court and continued the scrubbing procedures. However, whereas Judge Lamberth required only that he be notified of applications that contained Stellar Wind information, Judge Kollar-Kotelly required that such information be removed. ~~(TS//STLW//SI//OC/NF)~~

As described in Chapter Four, on March 14, 2004, OIPR Counsel Baker briefed Judge Kollar-Kotelly about the President's decision to sign the March 11, 2004, Presidential Authorization without the Justice Department's certification as to the Authorization's form and legality, and about subsequent changes the Authorization made to the Stellar Wind program. ~~(TS//SI//NF)~~

According to a handwritten letter Judge Kollar-Kotelly drafted to Baker following this meeting, Baker had informed her that the Stellar Wind program [redacted] The letter also stated that Baker informed her that with these changes the Deputy Attorney General agreed to certify the program as to form and legality, and that OLC had prepared a new legal memorandum regarding the legality of Stellar Wind to replace the November 2001 memorandum authored by Yoo. ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly's letter marked the first time her expectations concerning the Department's use of Stellar Wind information in FISA applications was communicated in writing to OIPR. Judge Kollar-Kotelly wrote,

> Although the Court has every confidence in the oral representations of Jim Baker [and] does not have any reason to question his honesty or credibility with the FISC or this judge, I am requesting that representations, previously done orally, now be put in writing that relate to [Stellar Wind] and FISA applications so that there are no misunderstandings.
>
> . . . .
>
> I want to emphasize my position which has been consistent since I came on the FISC in May 2002, the [Stellar Wind] program and FISA applications are to be kept separate, and no

> information direct or indirect, derived or obtained from [Stellar Wind] should be included in FISA applications. Only in this way can the integrity of the process and intelligence collected through FISA applications be maintained.
> ~~(TS//STLW//SI//OC/NF)~~

Judge Kollar-Kotelly also wrote that she would not sign any FISA applications that contained substantive information from Stellar Wind-generated tips or any applications where the Stellar Wind tip was the sole or principal factor for an agency initiating the underlying investigation, "even if the investigation was conducted independently of the tip from [Stellar Wind]." ~~(TS//STLW//SI//OC/NF)~~

Baker told us that this letter was Judge Kollar-Kotelly's preliminary response to the changes in the Stellar Wind program. Through subsequent discussions between Judge Kollar-Kotelly and Baker, and between Baker and other Department and FBI officials, a more flexible arrangement was reached on scrubbing that addressed Judge Kollar-Kotelly's concerns without imposing an absolute prohibition on including certain Stellar Wind-derived information in FISA applications.[347]
~~(TS//STLW//SI//OC/NF)~~

In short, the scrubbing procedures implemented in March 2004, and that continue to the present day, substantially expanded the procedures OIPR originally developed in February 2002.[348] In addition to determining whether any NSA information contained in international terrorism FISA applications was derived from Stellar Wind and whether there was any dual coverage, Judge Kollar-Kotelly required the FBI to determine whether any facility (telephone number or e-mail address) that appeared in a FISA application also appeared in a Stellar Wind report and, if so, whether the FBI had developed, independent of Stellar Wind, an investigative interest in the facility before it was the subject of an [redacted] tipper.[349] This third

---

[347] FBI OGC said that it was not until these discussions that the FBI was aware of the scrubbing procedures OIPR had implemented in approximately February 2002 after Judge Lamberth was read into the Stellar Wind program. ~~(TS//SI//NF)~~

[348] The scrubbing procedures described here apply both to NSA information derived from the Stellar Wind program and to information derived from the FISA Court's PR/TT and Section 215 bulk meta data orders. Until mid-2008 when the Stellar Wind program officially was closed, leads the NSA developed from the FISA-authorized bulk meta data collections were disseminated under the Stellar Wind compartment.
~~(TS//STLW//SI//OC/NF)~~

[349] As discussed in Chapter Three, Baker did not believe in May 2002, when he first discussed the subject with Judge Kollar-Kotelly, that such a scrub was possible. Baker told us that by March 2004 he better understood the NSA's and FBI's process for disseminating Stellar Wind information and the agencies' ability to track program-derived tips in a timely manner. ~~(TS//STLW//SI//OC/NF)~~

scrub is coordinated among OIPR, the FBI's National Security Law Branch (NSLB), and Team 10. ~~(TS//STLW//SI//OC/NF)~~

The scrub requires NSLB to compile a list of all "facilities" – telephone numbers and e-mail addresses – that appeared in any draft international terrorism FISA applications.[350] This list is compiled as FISA packages become ready for filing with the Court and is provided to an attorney in NSLB read into the Stellar Wind program. The attorney in turn forwards the facilities list to Team 10 at the NSA. Team 10 checks each facility against the NSA's Stellar Wind reports database to determine whether a listed facility is contained in any Stellar Wind reports and, if so, whether the facility appeared in the tearline portion of a report that was further disseminated to FBI field offices. If both inquiries are positive, Team 10 notes the date of the relevant Stellar Wind report and searches the FBI's Automated Case Support System (ACS) to determine whether the facility appears in ACS and, if so, the date the facility came to the FBI's attention. Team 10 reports the results of these checks to the NSLB attorney for review. ~~(TS//STLW//SI//OC/NF)~~

The NSLB attorney takes one of two steps at this stage. If Team 10's checks are negative – meaning none of the facilities are contained in a Stellar Wind report or contained in information below the tearline of a Stellar Wind report – the NSLB scrub attorney notifies the OIPR attorney and FBI case agent that the FISA application can be cleared for presentation to the FISA Court and that the application can proceed to final processing. If both checks on a facility are positive, the NSLB attorney will try to determine if there is a basis for the Court to allow the information in the application based on the theories, discussed in further detail below, that the FBI had an independent investigative interest in or would have inevitably discovered the facility in question. To determine this, the NSLB attorney researches FBI databases, analyzes records, and attempts to craft an argument under one of these theories. The NSLB attorney then provides this information to OIPR for presentation the Court. If the NSLB attorney cannot find a basis for including the information under either of the theories, and the facility is not essential to the showing of probable cause for the requested FISA coverage, the facility is excised from the FISA application, and processing continues. If the information is important to the probable cause showing, the NSLB attorney discusses with OIPR whether to make the argument to the appropriate FISA Court judge (initially

350 [redacted]

Judge Kollar-Kotelly and now, the judge assigned to case) that the facility nevertheless can remain in the application. ~~(TS//STLW//SI//OC/NF)~~

According to the Deputy General Counsel for NSLB, the argument to keep such information in an application is based on "standard Fourth Amendment [exclusionary rule] analysis." The "exclusionary rule" generally holds that where the government obtains evidence in violation of the Fourth Amendment, the court will suppress, or exclude, the evidence from the prosecutor's case-in-chief in a criminal trial. Under the "fruit of the poisonous tree" doctrine, a corollary to the exclusionary rule, any evidence obtained directly or derivatively from the government's improper conduct is also excluded. However, there are several exceptions to the exclusionary rule, two of which were relevant to scrubbing: independent source and inevitable discovery. The independent source exception holds that the exclusionary rule does not bar the use of evidence obtained in violation of the Fourth Amendment if there is also an independent, legal source for the evidence.[351] The inevitable discovery exception applies when evidence obtained in violation of the Fourth Amendment would have been obtained independently had the illegal search not occurred, which the government must prove by a preponderance of the evidence.[352] (U)

Thus, in the scrubbing context, the issue is whether the Stellar Wind information contained in a FISA application should not be excluded, either because the FBI had an investigative basis independent of Stellar Wind for including the information in the application or because the FBI inevitably would have discovered the information in the absence of Stellar Wind. More specifically, under the independent investigative basis exception, if Team 10's search of ACS shows that a facility came to the FBI's attention before the facility appeared in a Stellar Wind report, this fact establishes that the FBI has an independent, non-Stellar Wind factual basis to include the facility in the application.[353] NSLB Deputy General Counsel Thomas told us that in her experience the FBI already is aware of the facility – meaning it appears in ACS or other FBI databases – in nearly every instance that a facility contained in a FISA application also appears in a Stellar Wind report. ~~(TS//STLW//SI//OC/NF)~~

---

[351] See *Segura v. United States*, 468 U.S. 796, 805 (1984). (U)

[352] See *Nix v. Williams*, 467 U.S. 431, 443 (1984). (U)

[353] For example, in one case the NSLB attorney's review of the underlying investigative file showed that the FBI had obtained the telephone number at issue in response to an NSL Letter. Because the NSL was dated earlier than the Stellar Wind report that also contained the telephone number, the FBI had an independent investigative basis for including the number in the FISA application. ~~(TS//STLW//SI//OC/NF)~~

The inevitable discovery exception in the scrubbing context applies when Team 10's check of ACS indicates the FBI was not aware of the facility before the date of the Stellar Wind report containing the facility. Under this approach, the NSLB attorney attempts to demonstrate to OIPR that normal investigative steps in the underlying investigation inevitably would have identified the facility in question. The scrubbing attorney analyzes such case evidence as close associates and other relationships of the subjects of the investigation that could logically lead investigators – through NSLs, for example – to the facility contained in the Stellar Wind report.[354] ~~(TS//STLW//SI//OC/NF)~~

Until January 2006, when the full FISA Court was read into Stellar Wind, Judge Kollar-Kotelly required that all applications the FBI determined contained facilities or information that also appeared in Stellar Wind reports be cleared with her before being filed with the FISA Court. As she wrote in a January 12, 2005, letter to OIPR, "I want to ensure, that, to the extent possible, [Stellar Wind] information is excluded from applications submitted to the FISC and that, if it is necessary to include such information, it is specifically identified to the FISC as derived from [Stellar Wind] collection when the application is presented." OIPR Deputy Counsel Skelly-Nolen – who was read into Stellar Wind on March 12, 2004, but who had been involved in the scrubbing process since 2001 – was responsible, along with Baker, for coordinating this aspect of the scrubbing process and, when warranted, for presenting the argument to the judge that an application containing information that was the subject of a Stellar Wind report to the FBI should nevertheless be approved for filing. ~~(TS//STLW//SI//OC/NF)~~

Skelly-Nolen characterized the applications she presented to Judge Kollar-Kotelly as either "vanilla" or "non-vanilla." Vanilla applications were those for which Skelly-Nolen could confidently represent that the FBI had an independent investigative basis for the facility identified in the application that was the subject of a Stellar Wind report (for example, a facility the FBI learned of through FISA coverage that pre-dated the Stellar Wind report). Skelly-Nolen told us that over time Judge Kollar-Kotelly allowed the vanilla applications to be handled telephonically in an unclassified manner, a departure from her general requirement that the discussions be held in judge's chambers. Non-vanilla applications typically involved those cases that required Skelly-Nolan to demonstrate that the FBI

---

354 For example, in one case a telephone number of a particular business did not appear in an FBI database prior to the date it appeared in a Stellar Wind report. However, the subject of the underlying investigation was the target of an FBI national security investigation, and OIPR argued that the telephone number inevitably would have been connected to the subject through the "natural course of the investigation," possibly from toll records associated with other telephone numbers used by the subject, trash covers and open source information, or physical surveillance. ~~(TS//STLW//SI//OC/NF)~~

inevitably would have discovered the facility in question during the normal course of investigation. Skelly-Nolen said these cases were always discussed with Judge Kollar-Kotelly in person. ~~(TS//STLW//SI//OC/NF)~~

Skelly-Nolen told us that there were instances when Judge Kollar-Kotelly requested additional information to support the proffered theory for including Stellar Wind information in the FISA application. In some cases, Judge Kollar-Kotelly simply struck a line through the paragraphs in the filed application that contained the Stellar Wind-derived information and annotated in the margin, "This section (strike) not considered in evaluation of probable cause," followed by her signature and the date. Skelly-Nolen also said that in one or two cases Judge Kollar-Kotelly required that certain Stellar Wind information arguably necessary for establishing probable cause be removed from the applications.[355] However, in general Judge Kollar-Kotelly accepted OIPR's and the FBI's assessment that there was a non-Stellar Wind investigative basis for the information in question, or that the information inevitably would have been discovered even in the absence of Stellar Wind-derived tips to the FBI. ~~(TS//STLW//SI//OC/NF)~~

After operating under the expanded scrubbing procedures for approximately 6 months, Judge Kollar-Kotelly agreed in November 2004 to allow other FISA Court judges who had not yet been read into the Stellar Wind program to handle scrubbed international terrorism applications. However, Judge Kollar-Kotelly still required that Skelly-Nolen bring to her attention all vanilla and non-vanilla applications so they could be "cleared" before being formally filed. As noted above, it was not until January 2006, when the full FISA Court was read into Stellar Wind, that Skelly-Nolen was able to discuss such cases with other judges. ~~(TS//STLW//SI//OC/NF)~~

Since that time, the basic scrubbing procedure described above has continued. The Office of Intelligence attorney primarily responsible for the process told us that each new FISA application that references a facility that was disseminated under Stellar Wind is brought to the attention of the judge assigned to the case.[356] However, with limited exceptions, the FISA Court judges do not require that the government inform them of renewal applications that contain such facilities so long as they were previously brought to the Court's attention in the initiation application or prior renewal applications. The Office of Intelligence attorney told us that the government

---

[355] According to Skelly-Nolen, Judge Kollar-Kotelly nevertheless allowed OIPR to file these applications and approved them. ~~(TS//STLW//SI//OC/NF)~~

[356] The Office of Intelligence Policy and Review (OIPR) became a part of the Department's National Security Division, which was created in September 2006. As of April 2008, OIPR was renamed the Office of Intelligence. (U)

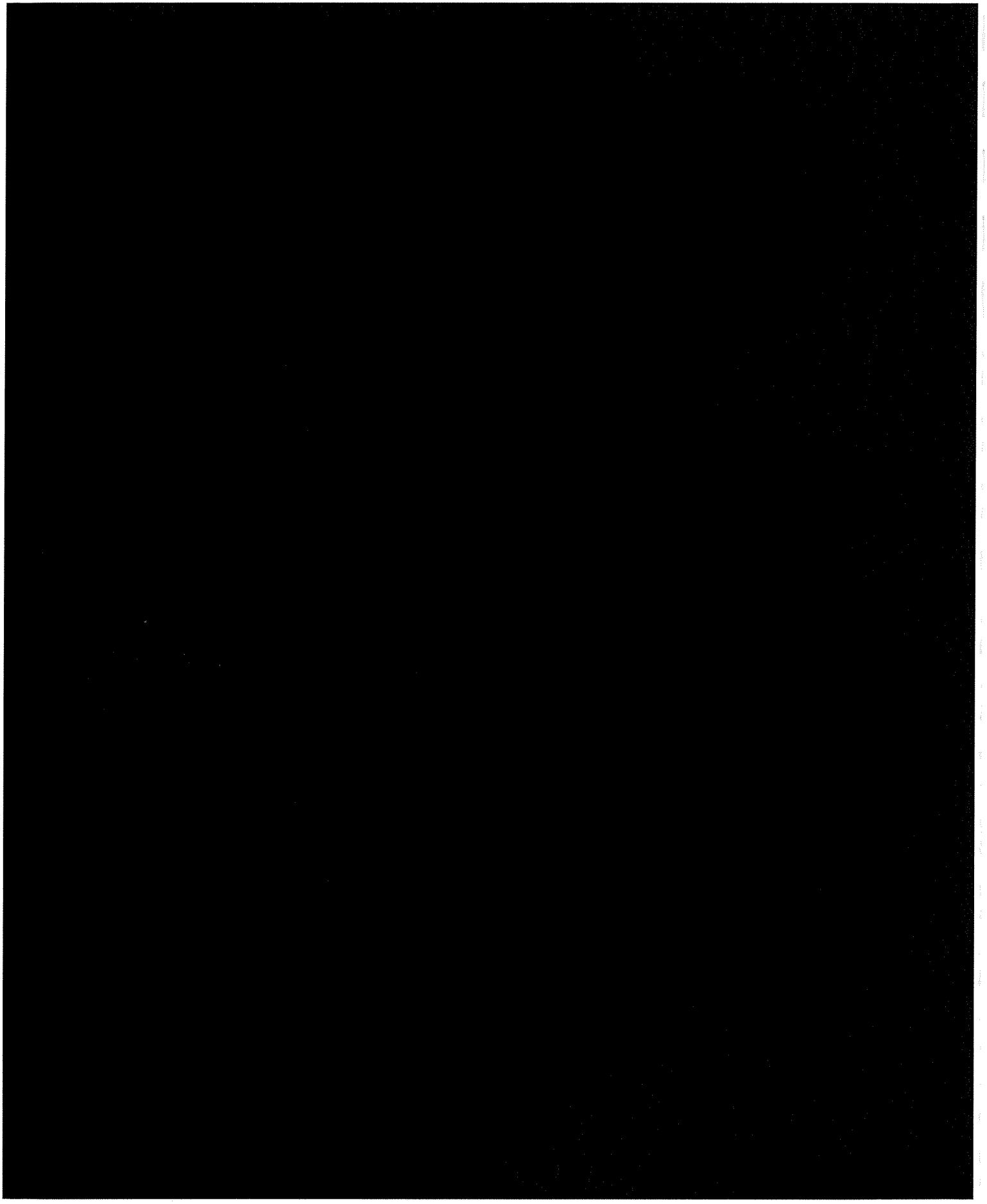
relies on the independent investigative interest theory in the majority of cases in which it seeks to keep a facility in an application. The attorney also said that from the perspective of the Office of Intelligence the scrubbing process is more manageable today than in the past because the process is better organized, additional personnel have been read into the program, and the FISA Amendments Act of 2008 extended the period of time the government must bring emergency applications to the FISA Court from 72 hours to 7 days. However, from the FBI's perspective, the scrubbing process continues to be burdensome and requires a significant expenditure of time and other resources. ~~(TS//STLW//SI//OC/NF)~~

IV. Impact of Stellar Wind Information on FBI Counterterrorism Efforts ~~(S//NF)~~

This section examines the impact of the information obtained from Stellar Wind on FBI counterterrorism efforts. It first provides statistics concerning the number of tippers from Stellar Wind information – telephony, e-mail, and content – disseminated to FBI field offices through the [redacted] process. Next, it describes how FBI field offices generally investigated [redacted] tippers and the typical results of the investigations. This section then summarizes two statistical surveys of meta data tippers the FBI conducted in 2006 to assess the value of Stellar Wind to FBI operations, and describes observations about the program's value provided to us by FBI officials and employees in OIG interviews and contained in documents the OIG obtained during the course of this review. Finally, the section examines [redacted] FBI international terrorism investigations commonly cited as examples of Stellar Wind's contribution to counterterrorism efforts in the United States. ~~(TS//STLW//SI//OC/NF)~~

A. Stellar Wind/[redacted] Statistics ~~(TS//STLW//SI//OC/NF)~~

We reviewed FBI and NSA statistics relating to the Stellar Wind program. According to an NSA document, from October 1, 2001, to February 28, 2006, the NSA provided [redacted] telephone numbers and e-mail addresses under the Stellar Wind program. The FBI disseminated most of these as tippers to field offices. Chart 6.1 depicts the distribution of the telephone numbers and e-mail addresses the NSA provided the FBI by type. ~~(TS//STLW//SI//OC/NF)~~



As described in Chapter Three, the NSA provided ratings, or [redacted] for each telephone number and e-mail address to help the FBI prioritize the tippers being disseminated to field offices. The FBI defined the rankings in ECs disseminated to field offices in the following manner:

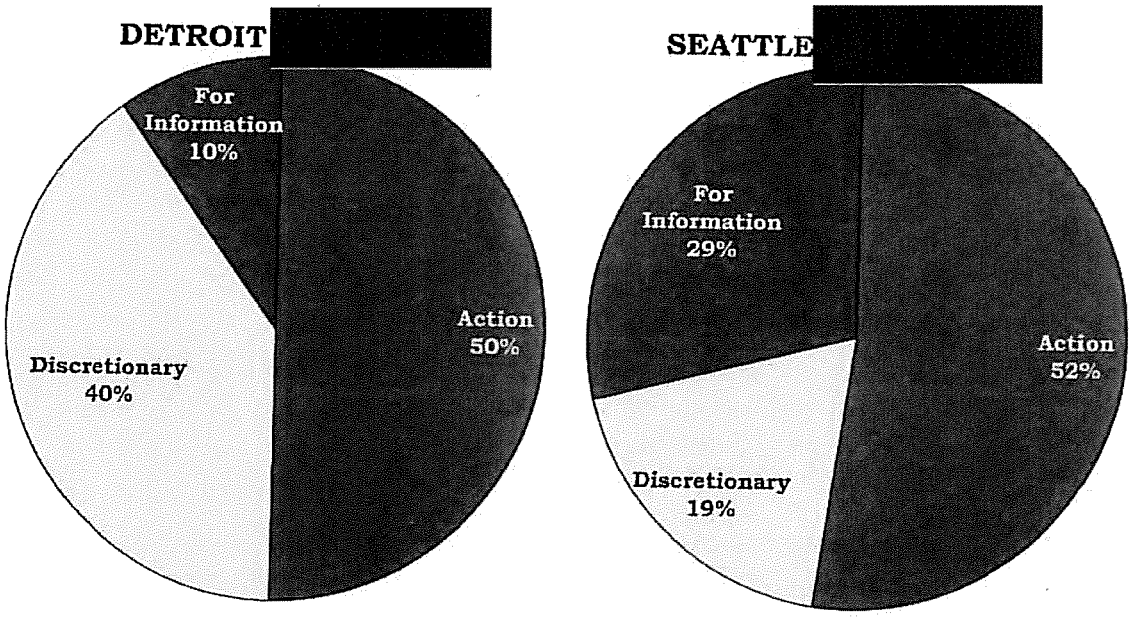
[redacted]

The FBI included these rankings in [redacted] and [redacted] ECs until early 2003. At that time, Team 10 began to make independent assessments about tippers' priority for the FBI, set leads on that basis, and generally discontinued including the ratings in [redacted] ECs. As discussed in this chapter, Team 10 usually set Action leads for telephone numbers and e-mail addresses the FBI did not already know and Discretionary leads for those the FBI was aware of in connection with closed or ongoing cases. ~~(TS//STLW//SI//OC/NF)~~

We could not compare the relationship between the NSA's [redacted] and the FBI's leads because the FBI did not maintain statistics about the lead type for each tipper that Team 10 disseminated. However, in connection with our visits to the FBI's Detroit and Seattle field offices, we examined the number of individual telephone numbers and e-mail addresses provided to those offices and the type of lead assigned for each. We determined that FBI Headquarters assigned Action leads for approximately 50 percent of the total [redacted] leads sent to these offices. As depicted in Chart 6.2, of the [redacted] leads sent to the Detroit field office from December 2001 to December 2006, [redacted] as Action leads. During this same period, of the [redacted] leads sent

to the Seattle field office, [redacted] as Action leads. These figures, taken together with the fact that only 5 percent of the meta data leads the NSA provided the FBI from October 1, 2001, to February 28, 2006, were rated [redacted], indicate that FBI field offices were required to investigate a substantial volume of telephone numbers and e-mail addresses that NSA analysts had rated [redacted] in terms of their connections to terrorism. ~~(TS//STLW//SI//OC/NF)~~

CHART 6.2: Percentage of Lead Types for Detroit and Seattle (January 2001 to May 2007) ~~(S//NF)~~
(Chart below is ~~SECRET//NOFORN~~)



With respect to leads that provided the content of communications the NSA intercepted under Stellar Wind, the manner in which these leads were disseminated depended on the nature of the communication. [redacted]

[redacted].[357] The FBI did not maintain statistics on the number of [redacted] content tippers disseminated to FBI field offices from Stellar Wind content reports. ~~(TS//STLW//SI//OC/NF)~~

We also found that [redacted] leads were distributed unevenly among FBI field offices. The majority of tippers were disseminated to large offices with substantial counterterrorism programs, such as New York, Washington, Chicago, and Los Angeles, and to offices whose territory contained significant Middle Eastern populations, such as Detroit. For example, FBI records indicate that of the [redacted] leads disseminated in 2005, 50 percent were assigned to 10 field offices. Table 6.1 depicts the distribution of [redacted] in 2005 among FBI field offices.[358] ~~(TS//STLW//SI//OC/NF)~~

TABLE 6.1: [redacted] Leads by Division (2005) (U//~~FOUO~~)
(Table below is ~~SECRET//NOFORN~~)

[redacted]

[357] [redacted]

[358] A "lead" in these figures does not equate to a single telephone number or e-mail address; each [redacted] lead could contain several telephone numbers or e-mail addresses. For example, the Detroit field office received [redacted] in 2005 containing [redacted] individual tippers. ~~(TS//STLW//SI//OC/NF)~~

[redacted]

B. FBI Field Office Investigations of [redacted] Tippers ~~(S//NF)~~

FBI field offices were not required to investigate every tipper disseminated under [redacted][359] Rather, the type of lead that the [redacted] EC assigned – Action, Discretionary, or For Information – governed a field office's response to a tipper.[360] [redacted] content tippers, which

---

[359] As discussed in Chapter Three, the practice under the [redacted] in the first several weeks of the Stellar Wind program was to set Action leads for all telephone number tippers. This practice was modified when the NSA began to designate each tipper in a Stellar Wind report [redacted]
~~(TS//STLW//SI//OC/NF)~~

[360] An Action lead instructs a field office to take a particular action in response to the EC. An Action lead is "covered" when the field office takes the specified action or conducts appropriate investigation to address the information in the EC. A Discretionary lead allows the field office to make a determination whether the information provided warrants investigative action. A field office that receives a "For Information" lead is not expected to take any specific action in response to the EC, other than possibly route the

(Cont'd.)

provided information derived from communications of telephone numbers and e-mail addresses under surveillance, generally assigned Discretionary or For Information leads. The information in these tippers usually related to individuals already under FBI investigation and was provided to the agents responsible for those cases. [redacted] e-mail address tippers generally assigned Discretionary leads to field offices unless the information was particularly urgent. As noted above, content and e-mail address tippers accounted for a comparatively small portion of the [redacted] tippers disseminated by Team 10. ~~(TS//STLW//SI//OC/NF)~~

The vast majority of FBI investigative activity related to Stellar Wind information involved responding to [redacted] telephone number tippers that assigned Action leads. Team 10 generally assigned Action leads for telephone numbers that the FBI did not previously know or that Team 10 otherwise deemed a high priority, such as a number that had a relationship to a major FBI investigation.[361] From approximately September 2002 (when [redacted] was created) to July 2003, Action leads instructed field offices to obtain subscriber information for the telephone numbers within its jurisdiction and to conduct any "logical investigation to determine terrorist connections." However, some agents complained that these Action leads lacked guidance about how to make use of the tippers, particularly given concerns that the [redacted] communications provided insufficient predication to open national security investigations. ~~(TS//STLW//SI//OC/NF)~~

Two changes in 2003 addressed some of these complaints. First, in July 2003 the CAU assumed responsibility from field offices for issuing NSLs, as we discussed in Section II above. Second, in October 2003 the Attorney General issued new guidelines for FBI national security investigations that created a new category of investigative activity called a "threat assessment."[362] [redacted]

---

communication to the office personnel whose investigations or duties the information concerns. ~~(S//NF)~~

[361] Discretionary leads were assigned to telephone numbers that already were known to the FBI, meaning the number or the number's subscriber was referenced in an active FBI investigation. These leads identified the case number of the related investigation and advised receiving field offices to "use the information as deemed appropriate" to bring the information to the attention of the appropriate case agent. ~~(S//NF)~~

[362] As noted earlier, the October 2003 guidelines, entitled Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI guidelines), replaced the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations. In September 2008, the Attorney General issued Guidelines for Domestic FBI Operations that replaced the October 2003 NSI guidelines with respect to domestic operations. The September 2008 guidelines use the term "assessment" instead of "threat assessment." (U)

[redacted] Thus, beginning in October 2003, Action leads assigned by [redacted] telephone number tippers instructed field offices to conduct threat assessments. ~~(TS//STLW//SI//OC/NF)~~

During our review, we visited the Detroit and Seattle field offices to review their handling of [redacted] leads. In addition, we interviewed several supervisory special agents at FBI Headquarters who had experience handling the leads in their respective field offices before being read into the program. In general, these agents' and analysts' experience with [redacted] leads was unremarkable. A threat assessment conducted by these agents and analysts typically involved querying several FBI, public, and commercial databases for any information about the tipped telephone number, and requesting that various state and local government entities conduct similar queries. Sometimes these queries identified the subscriber to the telephone number before the CAU obtained the information with an NSL. In other cases, the threat assessments continued after the field office received the NSL results.[363] ~~(TS//STLW//SI//OC/NF)~~

Examples of the databases utilized in their threat assessments included FBI systems such as the Automated Case Management System and [redacted] other government databases, such as the [redacted] state [redacted] databases, and local police department databases; and commercial databases, such as [redacted] The results of their checks of these databases could sometimes be extensive and include personal information not only about the subscriber to the tipped telephone number, but also about individuals residing in the subscriber's residence or other acquaintances. In other cases, checks were negative or revealed little information about the number or the subscriber. ~~(S//NF)~~

---

[363] We were told that it sometimes took [redacted] for field offices to receive subscriber information from the CAU. A Team 10 supervisor said field offices frequently contacted the CAU about the status of outstanding NSLs because the usefulness of threat assessments conducted on a telephone number were limited without the identity of the subscriber. ~~(S//NF)~~

The agents and analysts said they reviewed the results of these database checks to determine whether additional investigative steps under the threat assessment were warranted or whether there was predication to open a preliminary inquiry. None of the agents we interviewed could recall initiating any investigations based on a threat assessment of an [redacted] tipper.[364] They said they frequently closed [redacted] leads after conducting a threat assessment interview of the subscriber and determining that there was no nexus to terrorism or threat to national security. Alternatively, the leads were closed based solely on the results of database checks. ~~(TS//SI//NF)~~

Under the Attorney General's October 2003 national security investigations guidelines, [redacted] Under [redacted] agents were not permitted to explain to subscribers how they obtained the information that caused them to seek an interview. Instead, agents simply asked subscribers about their contacts in certain countries and with specific telephone numbers. Agents told us that subscribers generally consented to these interviews and were cooperative and forthcoming. In a few cases, subscribers refused the request or sought the advice of counsel.[366] ~~(TS//STLW//SI//OC/NF)~~

---

[364] Prior to the CAU's July 2003 decision to assume responsibility for issuing NSLs, agents in FBI field offices often opened investigations in order to issue NSLs to obtain subscriber information. These cases usually were closed after the agents conducted investigations and determined the domestic telephone number tipper did not have a nexus to terrorism. ~~(S//NF)~~

[365] On September 29, 2008, the Attorney General issued new guidelines for domestic FBI operations, which includes national security investigations. These guidelines [redacted] *Compare* Attorney General's Guidelines for Domestic FBI Operations, Section II.A.4.f. (September 29, 2008), *with* Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, Section II.A.6. (October 31, 2003). ~~(S//NF)~~

[366] Several of the threat assessment interviews that agents described to us and that we reviewed in FBI documents provided examples of how some domestic telephone numbers appeared on their face to be in contact with an individual involved in terrorism. In the Seattle field office, several interviews revealed that the foreign telephone calls placed to domestic numbers were made using a pre-paid telephone service from local stores because the callers, often relatives of the domestic contacts, did not have telephone service at their residences. Thus, while the intelligence indicating that an individual involved in terrorism used the foreign telephone number might have been accurate, the number also was used by individuals about whom there was no reason to believe were involved in terrorism. ~~(TS//STLW//SI//OC/NF)~~

FBI field offices were required to report the results of the threat assessments to the CAU. In most of the ECs we reviewed, the field offices reported all of the information that was located about the telephone numbers, including the details of any subscriber interviews, and then stated that the office determined the tipped telephone number did not have a nexus to terrorism and considered the lead closed. Much less frequently, field offices reported that a preliminary investigation was opened to conduct additional investigation.[367] Regardless of whether any links to international terrorism were identified, the results of any threat assessments and the information that was collected about subscribers generally were reported in communications to FBI Headquarters and uploaded into FBI databases. ~~(S//NF)~~

C. FBI Statistical Surveys of [redacted] Meta Data Tippers ~~(TS//STLW//SI//OC/NF)~~

The FBI made several attempts, both informal and more formal, to assess the value of Stellar Wind to FBI counterterrorism efforts. The first was an informal attempt by the FBI's OGC. FBI General Counsel Valerie Caproni told us that in early 2004 she spoke with the CAU Unit Chief and the Section Chief for the Communications Exploitation Section about trying to assess the value of Stellar Wind information. According to Caproni, the two managers stated that based on anecdotal and informal feedback from FBI field offices, the telephony meta data tippers were the most valuable intelligence from the program for agents working on counterterrorism matters. However, Caproni told us it was difficult to conduct any meaningful assessment of the program's value in early 2004 because FBI field offices at that time were not required to report to FBI Headquarters the investigative results of the Stellar Wind leads disseminated under [redacted] FBI Headquarters did not make such reporting mandatory until October 2004. As a result, Caproni's discussions with the FBI managers did not result in any written assessment of the program. ~~(TS//STLW//SI//OC/NF)~~

---

[367] The CAU advised field offices that investigative feedback about [redacted] tippers was important because it informed the "reliable source's" (the NSA's) assessment of whether to continue analyzing the "foreign entity" that caused the tippers to be disseminated. An NSA official told us that such information was also important to improving the NSA's analytical process, but he said it was sometimes difficult to obtain such feedback. A CAU Unit Chief told us that the NSA expressed particular concern about insufficient feedback from the FBI regarding investigative results pertaining to the tippers' nexus to terrorism. He said this was a difficult situation in that [redacted] professed to be sending out high value information about known links to terrorism," and it was "uncomfortable" to receive little feedback from field offices other than, "You're sending us garbage." Members of Team 10 told us that efforts to improve field office feedback over time had mixed results. ~~(TS//STLW//SI//OC/NF)~~

The FBI's second informal assessment of the value of Stellar Wind came after the December 2005 New York Times articles that publicly disclosed the content collection aspect of the Stellar Wind program. Caproni said that in preparation for Director Mueller's testimony at congressional hearings in 2006 on the issue, she attempted to evaluate the Stellar Wind program. Caproni stated that because NSA Director Hayden asserted publicly that the program was valuable, she wanted Mueller's testimony to identify, if possible, any investigations that illustrated Stellar Wind's positive contribution to the FBI's counterterrorism efforts. Caproni stated that this effort was complicated by the fact that Mueller's testimony would be limited only to the aspect of the program disclosed in the New York Times article and subsequently confirmed by the President – the content collection basket. ~~(TS//STLW//SI//OC/NF)~~

As discussed above, Caproni said that FBI field offices did not find this aspect of the program to be as useful as the telephony meta data, primarily because [redacted] was comparatively small and the FBI had FISA coverage on many of these already. Caproni told us that ultimately she was able to identify "a couple" of content tippers that contributed to FBI investigations, but she commented that there were not many. ~~(TS//STLW//SI//OC/NF)~~

The FBI subsequently conducted two more efforts to study the Stellar Wind program's impact on FBI operations, both in early 2006. The first study sampled the [redacted] tippers the FBI had received under Stellar Wind from 2001 through 2005. The second study reviewed [redacted] e-mail tippers the NSA provided the FBI from August 2004 through January 2006. In both of these studies, the FBI sought to determine what percentage of tippers resulted in "significant contribution[s] to the identification of terrorist subjects or activity on U.S. soil." We describe in the next sections the findings of these two studies.
~~(TS//STLW//SI//OC/NF)~~

1. Early 2006 Survey [redacted] Telephony and E-Mail Meta Data Tippers ~~(TS//STLW//SI//OC/NF)~~

Following the December 2005 New York Times article publicly disclosing the content collection aspect of Stellar Wind, additional members of the Senate and House Intelligence Committees were read into the program. During this time, the NSA provided to cleared members of Congress substantive briefings about Stellar Wind, and the FBI was asked to testify about its participation in the program. In preparation for these briefings and testimony, the FBI sought to quantify the value of Stellar Wind intelligence for FBI counterterrorism operations. The CAU conducted a statistical study for this purpose, and in May 2006 the FBI provided a copy

of the statistical report to the Senate Select Committee on Intelligence. ~~(TS//STLW//SI//OC/NF)~~

The study, conducted during a 1-week period in January 2006, sampled [redacted] unique telephone numbers and e-mail addresses the NSA provided the FBI from the inception of the Stellar Wind program through 2005.[368] The study sought to determine what percentage of the tippers resulted in "significant contribution[s] to the identification of terrorist subjects or activity on U.S. soil." Working with an FBI statistician, the CAU determined that [redacted] randomly selected tippers would be required to obtain statistically significant results. ~~(TS//STLW//SI//OC/NF)~~

Approximately 30 analysts from the FBI's Counterterrorism Division were assigned the task of reviewing [redacted] tippers to determine the disposition of each.[369] The analysts sought to determine whether a particular tipper made a "significant" contribution to FBI counterterrorism efforts. For purposes of the study, a tipper was considered "significant if it led to any of three investigative results: the identification of a terrorist, the deportation from the United States of a suspected terrorist, or the development of an asset that can report about the activities of terrorists." A tipper that led to a field office opening a preliminary or full investigation was not considered "significant" for purposes of the study. ~~(TS//STLW//SI//OC/NF)~~

The analysts researched each tipper's disposition in investigative records contained in FBI electronic databases, beginning with the [redacted] EC that disseminated the tipper to the field. If an analyst concluded based on this research that a tipper was significant, a second analyst who was familiar with the Stellar Wind program further reviewed that determination. If the CAU analyst agreed with the initial finding, the tipper

---

[368] According to the CAU report, the NSA had provided the FBI [redacted] tippers since the inception of Stellar Wind, but [redacted] were duplicates. [redacted] was the total number of unique tippers. The tippers by year were broken down as follows: [redacted] The study also did not include content tippers. ~~(TS//STLW//SI//OC/NF)~~

[369] Most of the analysts were not read into the Stellar Wind program and were told that the study concerned the disposition of [redacted] leads. Of [redacted] tippers reviewed by the analysts, approximately 12 percent were e-mail addresses, a figure consistent with the overall tipper breakdown between e-mail addresses and telephone numbers. ~~(TS//STLW//SI//OC/NF)~~

and supporting information was presented to the CAU Unit Chief for a final review.[370] ~~(TS//STLW//SI//OC/NF)~~

Based on this methodology, the study found that [redacted] 1.2 percent, of [redacted] tippers were "significant." The study extrapolated this figure to the entire population of [redacted] tippers and determined that one could expect to find [redacted] tippers the NSA provided the FBI under Stellar Wind were significant. ~~(TS//STLW//SI//OC/NF)~~

The report documenting the study's findings included brief descriptions of [redacted] "significant" tippers. For example, according to the report, one tipper led to the opening of a full investigation that developed evidence that the user of the tipped e-mail address had "definite ties to terrorism." The user was arrested and pled guilty to charges of [redacted] Another tipper led to the identification of an individual who, [redacted] ~~(TS//STLW//SI//OC/NF)~~

Several of the "significant" tippers related to ongoing FBI investigations. For example, information from one tipper designated as significant was already known to the relevant FBI field office, which had an investigation ongoing concerning a subject associated with the tipper prior to receiving the [redacted] EC. According to the study's brief description of the case's significance, the investigative file stated that the tipper was "very beneficial in the on-going investigation" by connecting the subject to terrorism, without describing that connection. Another tipper caused a field office to change a preliminary investigation to a full investigation regarding the possible illegal [redacted] The tipper indicated a connection between one of the subjects of the preliminary investigation and a known terrorist. ~~(TS//STLW//SI//OC/NF)~~

The study also found that 28 percent of [redacted] tippers were never disseminated to FBI field offices for investigation. According to the report, the CAU filtered out these tippers based on "lack of significance" when they were first provided to the FBI by the NSA. These tippers were deemed non-significant for purposes of the study. In addition, the study found that for 22 percent of the sample tippers, FBI field offices did not report any

---

[370] According to a CAU analyst closely involved with the study, establishing a fairly "tight" criteria to identify "significant" tippers was necessary in order to obtain statistically significant results within the one-week time frame the CAU was given to complete the review. The analyst told the OIG that analysts initially applied a broader "significant" standard in their reviews of the tippers, but that it immediately became apparent that a stricter standard was required. The Unit Chief for the CAU told the OIG that the definition of "significant" ultimately used for the study was reached by consensus among Counterterrorism Division operational and analytical personnel. ~~(S//OC/NF)~~

investigative results. The study assumed that the field offices investigated the leads that were set but did not document their work in ACS. These tippers were deemed non-significant for purposes of the study.[371] Thus, combining these two categories, approximately 50 percent of the tippers reviewed as part of the CAU study either were never disseminated to FBI field offices, or were disseminated but with unknown investigative results.[372] ~~(TS//STLW//SI//OC/NF)~~

The FBI's report of the study did not explicitly state any conclusions about whether Stellar Wind was a valuable program. FBI OGC told the OIG that based in part on the results of this study, which found [redacted] of the leads were significant, FBI executive management concluded that the program was "of value." The FBI OGC also said that FBI Director Mueller and Deputy Director Pistole provided congressional testimony in February and May 2006, respectively, about the value of the program, which the FBI OGC stated was based in part on the results of the study. ~~(TS//STLW//SI//OC/NF)~~

2. January 2006 Survey [redacted] E-Mail Meta Data Tippers ~~(TS//STLW//SI//OC/NF)~~

The CAU conducted a second study of Stellar Wind tippers in January 2006. According to Caproni, this study was in response to a request from the FISA Court about intelligence being obtained pursuant to the July 14, 2004, Pen Register/Trap and Trace Order that authorized the bulk collection of e-mail meta data. As discussed in Chapter Five, e-mail meta data was the first basket of Stellar Wind's signals collection activity that was placed under the FISA Court's authority. However, as noted earlier, the

---

[371] As noted, Caproni cited this lack of reporting from field offices as a reason for not being able to conduct a meaningful assessment of the Stellar Wind program's value in the spring of 2004. FBI Headquarters did not officially require field offices to report investigative results concerning [redacted] tippers until October 2004. According to the CAU analyst with whom the OIG spoke about the study, the idea of contacting field offices to discuss the disposition of tippers and to seek general observations about [redacted] was rejected because of the concern the inquiries might expose the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

[372] By its methodology, the only tippers the study assessed for "significance" were those for which field offices reported investigative results to the CAU and therefore generally did not take into account tippers assigned as Discretionary leads. Discretionary leads, as distinguished from Action leads, did not require field offices to report to the CAU about how the tippers were used. Yet, according to FBI personnel, these leads sometimes were associated with ongoing investigations and sometimes provided new or additional indications of terrorist connections, or reported the content of communications indicating a subject's international movements. The "value" of this category of tippers was not captured in the FBI's study. ~~(TS//STLW//SI//OC/NF)~~

NSA continued to provide e-mail addresses to the FBI in Stellar Wind reports. ~~(TS//STLW//SI//OC/NF)~~

This second study, which reviewed each [redacted] e-mail tippers the NSA provided the FBI from August 2004 through January 2006, applied the same methodology for assessing "significance" that was used in CAU's first study. The second study found that none [redacted] e-mail tippers was "significant" under this standard. The report noted, however, that many of the investigations related to the reviewed e-mail tippers were still ongoing. In addition, the study observed that some of the tippers reviewed had only recently been disseminated to field offices for investigation and that it was possible investigation of these tippers had not been completed. ~~(TS//STLW//SI//OC/NF)~~

D. FBI Judgmental Assessments of Stellar Wind Information ~~(S//NF)~~

To attempt to further assess the value of Stellar Wind information for the FBI, we interviewed FBI Headquarters officials and employees who regularly handled Stellar Wind information. We also interviewed personnel in FBI field offices who were responsible for handling [redacted] tippers. We asked these witnesses for their assessments of the impact of Stellar Wind or [redacted] information on FBI counterterrorism operations. We also recognize that FBI officials and agents other than those we interviewed may have had experiences with [redacted] different than those summarized below. ~~(TS//STLW//SI//OC/NF)~~

The members of Team 10 and its predecessor [redacted] were strong advocates of the program and stated that they believed it contributed significantly to FBI international terrorism investigations. Several claimed that program tippers helped the FBI identify previously unknown subjects, although they were not able to identify for us any specific cases where this occurred. Other witnesses cited the FBI's increased cooperation with the NSA on international terrorism matters as a side benefit of the Stellar Wind program.[373] ~~(TS//STLW//SI//OC/NF)~~

FBI officials and agents from the International Terrorism and Operations Section (ITOS) expressed a more moderate assessment of Stellar Wind. None of the ITOS officials we interviewed could identify significant investigations to which Stellar Wind substantially contributed. However,

---

[373] FBI Deputy General Counsel Julie Thomas also said that Stellar Wind helped improve the relationship between the FBI and CIA. She said the program provided an opportunity to demonstrate the "interoperability of different agencies," and based on her experience dealing with program-related matters the relationship between the FBI and the NSA was "better now than it has ever been." ~~(TS//STLW//SI//OC/NF)~~

they were generally supportive of the program, often stating that it was "one tool of many" in the FBI's fight against international terrorism. ~~(TS//SI//NF)~~

ITOS personnel frequently noted for us the deficiencies in the Stellar Wind information disseminated to field offices, such as the lack of details about the foreign individuals allegedly involved in terrorism with whom domestic telephone numbers and e-mail addresses were in contact. However, these FBI employees believed the possibility that such contacts related to terrorism made investigating the tips worthwhile. Some ITOS witnesses also told us that in their experience the FBI was already aware of many of the telephone numbers and e-mail addresses disseminated under [redacted] but that this duplication did not mean the information was without investigative value. For example, one witness said such contacts could "help move cases forward" by confirming a subject's contacts with individuals involved in terrorism or identifying additional terrorist contacts. ~~(TS//STLW//SI//OC/NF)~~

One FBI Headquarters supervisory special agent said that FBI field offices might have been less critical of [redacted] had there been agents in the offices read into Stellar Wind. He said that such agents would have been better positioned than FBI Headquarters' officials to assure others in their respective offices about the reliability of the information being disseminated. A former ITOS section chief told the OIG that he proposed to the NSA that the head of each FBI field office be read into Stellar Wind for this reason and to be able to make fully informed decisions about handling the Stellar Wind tippers. ~~(TS//STLW//SI//OC/NF)~~

The most critical comments we heard about [redacted] impact came primarily from the supervisory special agents we interviewed who managed counterterrorism programs at the two FBI field offices we visited. These agents said the [redacted] tippers and any information developed from the leads might be useful, but that the [redacted] program was not an effective way to identify threats. For example, one supervisor stated that [redacted] represented FBI Headquarters' failure to prioritize threat information. He said that by simply disseminating [redacted] tippers to field offices in ECs that often provided little in the way of details, FBI Headquarters effectively made the field offices "insurance carriers," placing the responsibility solely on them to timely and adequately investigate every lead. The supervisor stated that ordinarily he accepts this responsibility as part of his job, but that the [redacted] tippers were especially frustrating

as compared to other counterterrorism leads the office received because they did not provide sufficient information for him to prioritize the leads.[374]

Another supervisory special agent expressed a similar assessment of [redacted] stating that he felt the project "perverted the logical priority of tasking." He said that absent the leads' special status as part of [redacted] a very low percentage of the tippers would have been considered priority matters. He told us that he did not have the freedom to prioritize the leads in the manner he felt was warranted by the information provided in [redacted] ECs. ~~(TS//SI//NF)~~

Field office agents who investigated [redacted] leads also were critical of the lack of details contained in [redacted] ECs about the nature of the terrorist connection to the domestic contact, or about the contact itself, such as the duration or frequency of the calling activity. Some agents we interviewed said they also occasionally were frustrated by the prohibition on using [redacted] information in any judicial process, such as in FISA applications, although none could identify an investigation in which the restrictions adversely affected the case. ~~(TS//STLW//SI//OC/NF)~~

Most of the agents we interviewed viewed [redacted] tippers as just another type of lead that required appropriate attention, and the agents generally did not handle the leads with any greater care or sense of urgency than non-[redacted] counterterrorism leads. ~~(TS//SI//NF)~~

Moreover, none of the agents we interviewed identified an investigation in their office in which [redacted] played a significant role, nor could they recall how such a tipper contributed to any of their international terrorism cases. Nevertheless, the agents generally viewed [redacted] tippers as a potentially valuable source of information, noting that the information developed from the investigations of tippers might prove useful in the future. ~~(TS//SI//NF)~~

Agents also stated that through the threat assessment interviews they conducted of the subscribers to tipped telephone numbers, [redacted] "opened a window" to populations within the field offices' jurisdiction that

---

[374] The supervisor stated that [redacted] leads had little investigative value to his office. First, he said the leads did not provide enough detail about the reliability of the information being provided. Such details might include, for example, what other individuals had access to the foreign telephone allegedly used by someone involved in international terrorism, and how many calls were made from that number and for what durations. These details would help evaluate the threat represented by the foreign number's contact with the tipped domestic number. Second, the supervisor said the [redacted] tippers lacked direction about what the office should do with a tipped number after a threat assessment has been conducted. ~~(TS//SI//NF)~~

might not otherwise be as accessible. For example, [redacted] ~~(TS//STLW//SI//OC/NF)~~

In 2007, FBI Deputy Director John Pistole briefed the Senate Select Committee on Intelligence concerning the FBI's participation in the Stellar Wind program. A document prepared in connection with that briefing addressed, among other subjects, the program's value in FBI national security investigations. The document stated,

> [S]uccessful national security investigations are rarely the result of a single source of information. Rather they occur after exhaustive hours of investigation and the use of legal process in which bits and pieces of intelligence from many sources are gathered and combined into a coherent whole. The *success* or *effectiveness* of any intelligence program – whether Stellar Wind . . . or anything else – is sometimes difficult to assess in the abstract because of that blending of multiple strains of intelligence and because success should never be measured only in terms of terrorist plots that have visibly been disrupted, but also in plots that never formed because our investigative actions themselves had a disruptive effect. (Italics in original.)[375] ~~(TS//STLW//SI//OC/NF)~~

We interviewed FBI Director Mueller in connection with this review and asked him about the value of Stellar Wind to the FBI's counterterrorism program. FBI Director Mueller told us that he believes the Stellar Wind program was useful and that the FBI must follow every lead it receives in order to prevent future terrorist attacks. He said "communications are absolutely essential" to this task and called meta data the "key" to the FBI's

---

[375] A "talking points" document the FBI drafted for Director Mueller also expressed this view. The document stated:

> [The] impact of any single piece of intelligence or program is difficult to quantify. Combination of various information, including humint, sigint, and elsur, is necessary to address the global threat. Accordingly, it is not possible to make an unequivocal "but for" connection between a tip and any particular FBI investigation that has resulted in a seizure or arrest. However, the information has amplified, corroborated and directed FBI investigative resources. ~~(TS//STLW//SI//OC/NF)~~

communications analysis. Mueller also stated that to the extent such information can be gathered and used legally it must be exploited and that he "would not dismiss the potency of a program based on the percentage of hits." Asked if he was familiar with any specific FBI investigations that represent Stellar Wind successes, Mueller said that as a general matter it is very difficult to quantify the effectiveness of an intelligence program without "tagging" the leads that are produced in order to evaluate the role the program information played in any investigation. ~~(TS//STLW//SI//OC/NF)~~

We also asked Mueller about the issue of allocating finite FBI resources to respond to Stellar Wind leads. Mueller said that in the period after the September 11 terrorist attacks, the FBI remained in a state of continuous alert for several years. Mueller stated that he understood the President's desire to take every step to prevent another terrorist attack, and believes that it would be wrong not to utilize all available capabilities to accomplish this, so long as it is done legally. ~~(TS//STLW//SI//OC/NF)~~

Mueller also commented on media reports regarding FBI agents' frustration with the volume of [redacted] leads. For example, articles described complaints of unidentified FBI field agents regarding the lack of information in the tippers they received under [redacted] and how the high volume of tippers necessitated devoting significant resources to what were described as "dry leads."[376] Mueller said that the agents' frustration was similar to that expressed about other sources for the thousands of leads the FBI received after September 11, such as calls from citizens. Mueller stated that he understood the frustration associated with expending finite resources on numerous leads unlikely to have a terrorism nexus, but said that his philosophy after September 11 was that "no lead goes unaddressed." Moreover, he stated that frustrations can result from any counterterrorism program. ~~(S//NF)~~

We also interviewed Kenneth Wainstein, the first Assistant Attorney General for the Justice Department's National Security Division, which was created in September 2006. Wainstein told us that he was aware of "both sides" on the question of Stellar Wind's value. He also said that he heard the government had not "gotten a heck of a lot out of it," but noted that NSA Director Hayden and FBI Director Mueller have stated that the program was valuable. ~~(S//NF)~~

Hayden told us that he always felt the Stellar Wind program was worthwhile and successful. [redacted]

[376] See, e.g., Lowell Bergman, et al., "Domestic Surveillance: The Program; Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," The New York Times, January 17, 2006. (U)

[redacted] Hayden said the FBI believed the leads represented "something certain," when in fact the leads were only "narrow threads" and that the idea was to help build the FBI's intelligence base. Hayden also observed that the enemy may not have been as embedded in the United States as much as feared, but said that he believes Stellar Wind helped determine this. ~~(TS//STLW//SI//OC/NF)~~

E. Examples of FBI Counterterrorism Cases Involving Stellar Wind Information ~~(S//NF)~~

As part of our review, we sought to identify specific FBI international terrorism investigations in which Stellar Wind information was used and to describe the information's specific contributions to the investigations. We agree with FBI officials that this is a difficult task in view of the nature of these investigations, which frequently are predicated on multiple sources of information. To the extent Stellar Wind tips played a role in an investigation, the tips could be one of several sources of information acquired over time and used by the FBI to pursue the investigation. Moreover, the FBI agents and analysts we interviewed during our review could not say that "but for" a Stellar Wind tipper a given investigation would not have been productive, and they were unable to recall specifically how, if at all, Stellar Wind intelligence may have caused their investigations to take a particular direction. ~~(S//NF)~~

Our review did not seek to describe Stellar Wind's impact on each FBI field office, and we recognize that FBI officials and agents other than those we interviewed might have had experiences with [redacted] different than those summarized in this chapter. [redacted] Because such reporting was not disseminated to FBI field offices under [redacted] any contribution the information might have made to investigations FBI personnel we interviewed were familiar with might not have been accounted for in our questions about Stellar Wind and [redacted] information. ~~(TS//STLW//SI//OC/NF)~~

In view of these difficulties, we examined several investigations frequently cited in NSA and FBI documents the OIG obtained during this

review as examples of Stellar Wind information that contributed to the FBI's counterterrorism efforts.[377] For these investigations, we examined [redacted] ECs, FBI Letterhead Memoranda describing the status of investigative activities in specific cases, Counterterrorism Division responses to OIG questions about the role of [redacted] in specific investigations, government pleadings filed in international terrorism prosecutions, and FBI briefing materials.[378] ~~(TS//STLW//SI//OC/NF)~~

1. [redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[377] As noted above, the FBI was not the only customer of Stellar Wind information. The CIA and the National Counterterrorism Center also received Stellar Wind reports potentially relevant to their operations. Pursuant to a directive in the FISA Amendments Act of 2008, Intelligence Community OIGs are examining the impact Stellar Wind had on their respective agencies or if Stellar Wind information contributed to their agencies' operations. ~~(TS//STLW//SI//OC/NF)~~

[378] The briefing materials were prepared by the FBI's Communications Exploitation Section (CXS) shortly after aspects of the Stellar Wind program were publicly revealed in a series of New York Times articles in December 2005. The briefing materials were prepared at the direction of FBI General Counsel Valarie Caproni, who anticipated that Director Mueller and Deputy Director Pistole would be called to testify about the program. These briefing materials were intended to help prepare Mueller and Pistole for their testimony. The briefing materials include summaries of specific cases relating to Stellar Wind information that were highlighted by the NSA. ~~(TS//STLW//SI//OC/NF)~~

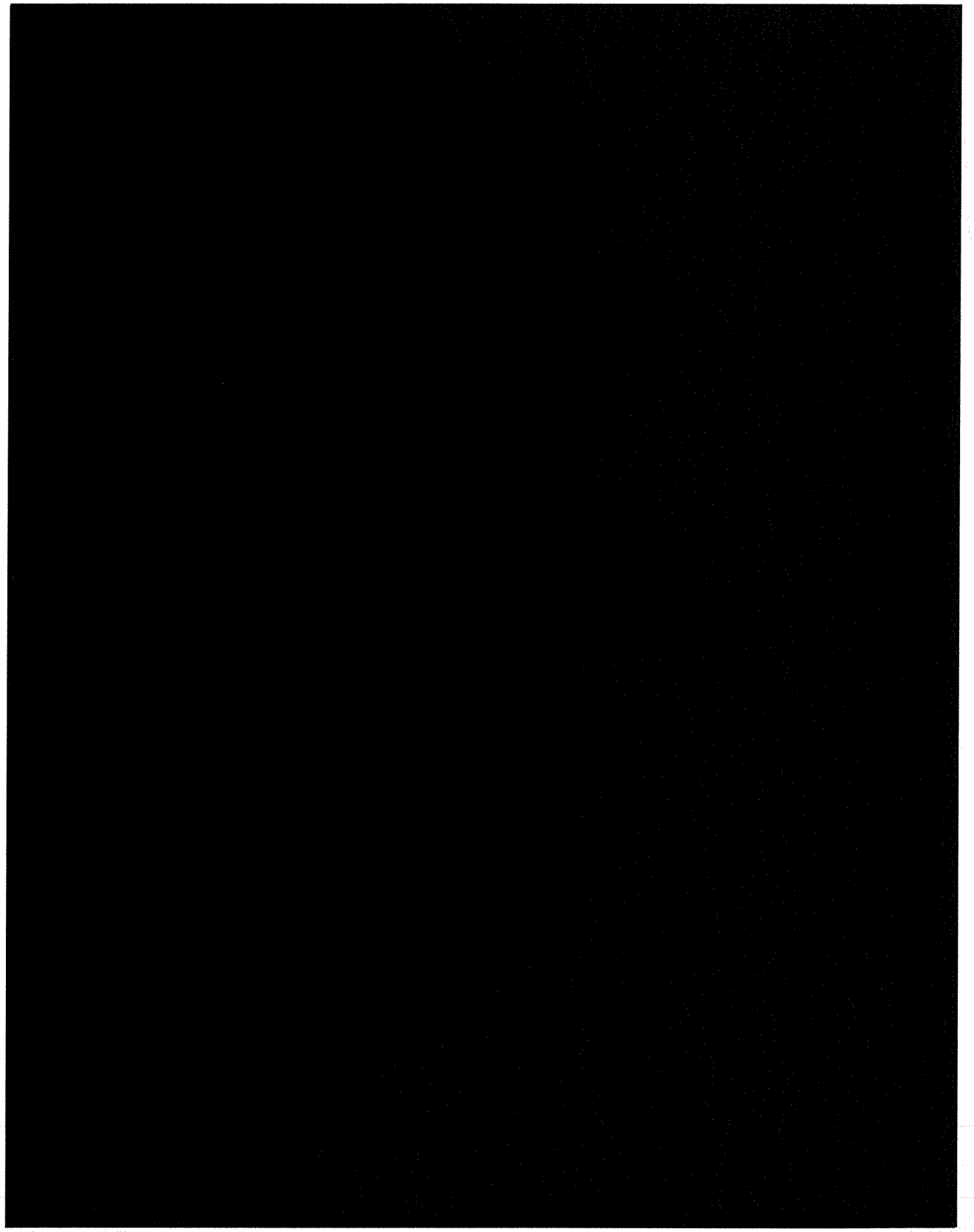
[redacted] This information generated several [redacted] leads for FBI field offices. ~~(TS//STLW//SI//OC/NF)~~

Several of these leads resulted in the FBI initiating investigations of [redacted] to identify any involvement in terrorism. In most cases, the FBI concluded that the individuals' connection [redacted] was not related to any involvement in terrorism. However, in one case FBI investigation determined that the individual was in contact with additional [redacted] engaged in activities indicating possible involvement in terrorist activities.[381] In another case, the FBI

[379] We described [redacted] in Chapter Three. ~~(S//OC/NF)~~

[380] [redacted]

[redacted][redacted][redacted][



However, according to documents provided to the OIG, the FBI was [redacted] The FBI therefore was unable to establish that there was a nationwide conspiracy [redacted] to provide material support to terrorism. ~~(S//OC/NF)~~

Nevertheless, FBI documents state that after [redacted] was closed, field offices with [redacted] -related investigations conducted "successful disruption operations" of criminal activities that were identified during the course of the investigations. ~~(S//OC/NF)~~

3. [redacted] **~~(TS//STLW//SI//OC/NF)~~**

[redacted]

The FBI's [redacted] opened a full investigation on [redacted] based on his statements [redacted] ~~(S//OC/NF)~~

Acting in coordination with [redacted] law enforcement and intelligence agencies, the FBI learned that a group of [redacted] This investigation came to be known by the code name [redacted][384] ~~(TS//SI//OC/NF)~~

[383] [redacted]

[384] [redacted]

[redacted]

[redacted]

[redacted] The EC set a discretionary lead for the FBI [redacted], but encouraged the field office to "provide any pertinent follow-up questions to . . . CAU, for submission to and consideration by the [redacted] source." ~~(TS//STLW//SI//OC/NF)~~

[redacted]

An FBI response to an OIG request for information about the role of [redacted] in [redacted] case stated that as a result of the [redacted] tipper, the [redacted] located [redacted] after [redacted] return to the United States and established surveillance on [redacted]. In an FBI document entitled [redacted]

---

[385] FBI documents we reviewed do not indicate how this information was obtained or whether it was derived from Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

[386] The briefing materials state that it could not be verified whether [redacted] ~~(S//OC/NF)~~

[redacted]" it is noted that at the time [redacted] returned to the United States the FBI had FISA coverage on [redacted] According to the document, [redacted][387] ~~(TS//STLW//SI//OC/NF)~~

FBI briefing materials state that the FBI first began surveillance of an individual later determined to be misidentified [redacted] Through open source investigation, the FBI obtained the telephone number of the misidentified subject and was granted emergency FISA authority on that number. FISA surveillance was initiated on the telephone believed to be used [redacted] ~~(TS//STLW//SI//OC/NF)~~

On [redacted] the FBI employees located at the NSA (Team 10) submitted a request to the NSA for call chaining analysis and consideration for Stellar Wind "tasking," or content collection. The NSA initiated content collection on the erroneous telephone number the same day. Contact chaining on the telephone number did not reveal any contacts with any known terrorist-associated numbers. On [redacted] it was determined [redacted] was not using the telephone number tasked and chained under Stellar Wind authority. The FBI also ceased FISA-authorized electronic surveillance of the number [redacted] By [redacted] ongoing physical surveillance confirmed that the telephone number believed to be associated [redacted] had been misidentified. ~~(TS//STLW//SI//OC/NF)~~

On [redacted] the primary suspects in the [redacted] were arrested. [redacted] ~~(S//OC/NF)~~

An FBI document stated that since [redacted] arrest [redacted] "has provided a wealth of intelligence to the FBI and the Intelligence Community," and that the intelligence [redacted] provided has been disseminated to intelligence services [redacted] ~~(S//OC/NF)~~

---

[387] A CXS intelligence analyst who drafted the summary of [redacted] for the CXS briefing materials told the OIG that she concluded that the FBI "probably would have figured out eventually" [redacted] was back in the United States based on [redacted] ~~(TS//STLW//SI//OC/NF)~~

On [redacted] pled guilty to [redacted] of [redacted] remains incarcerated [redacted]. ~~(S//NF)~~

[redacted]

According to a [redacted] FBI PowerPoint presentation about the FBI's role in Stellar Wind, the [redacted] tipper "facilitated the FBI's ability to locate, initiate physical surveillance, and debrief [redacted] in a timely manner." The facts reviewed by the OIG show that [redacted] failed to result in notification to the FBI of [redacted] return to the United States, but that through Stellar Wind information the FBI was able to locate [redacted] and obtain surveillance of [redacted] ~~(TS//STLW//SI//OC/NF)~~

4. [redacted] **~~(TS//STLW//SI//OC/NF)~~**

[redacted]

According to FBI briefing material, as a result of the [redacted] tipper the [redacted] opened a full international terrorism investigation on [redacted] (~~S//OC/NF~~)

[redacted]

After receiving the [redacted] tipper in [redacted] the [redacted] requested that FBI Headquarters apply for a FISA order to conduct surveillance of [redacted] The FBI subsequently obtained [redacted] and began FISA electronic surveillance [redacted] (~~TS//STLW//SI//OC/NF~~)

According to an [redacted] Letterhead Memorandum (LHM) drafted by the FBI case agent on [redacted] the FBI determined from [redacted] (~~TS//STLW//SI//OC/NF~~)

---

389 According to the EC, [redacted] interviewed in connection with the FBI's effort to ascertain [redacted] who the FBI suspected of having ties to [redacted] (~~S//NF~~)

390 According to the EC, the individual was reported to have told the police [redacted] (~~S//OC/NF~~)

[redacted]

The [redacted] LHM described other evidence seized [redacted] In addition, the LHM described additional evidence gathered through several detainee interviews [redacted] ~~(S//OC/NF)~~

The FBI arrested [redacted] and an associate [redacted] were indicted on [redacted] indicted on [redacted] ~~(S//NF)~~

The arrest and indictment arose out of [redacted] ~~(S//NF)~~

[redacted]

[redacted]

Following [redacted] trial, [redacted] was convicted on [redacted] [redacted].[393] He was sentenced to [redacted] prison term. ~~(S//NF)~~

In an undated summary of successes under the Stellar Wind program, the NSA characterized [redacted] as

[redacted]

[redacted]

[393] [redacted] was convicted on [redacted] against [redacted] ~~(S//NF)~~

The government's response to the [redacted] stated that the FBI initiated a national security-international terrorism investigation of [redacted] after receiving the [redacted] EC. The government stated that the [redacted] ~~(TS//STLW//SI//OC/NF)~~

5. [redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

The FBI closed its preliminary investigation of [redacted] after it concluded [redacted] had no nexus to terrorist activities. ~~(S//NF)~~

[redacted]

[redacted]

According to FBI briefing materials, based on the [redacted] investigation of [redacted] associates [redacted] a FISA order was obtained for [redacted] According to an FBI declaration filed in discovery litigation concerning [redacted] the [redacted] tipper in [redacted] investigation was not used to obtain the FISA order; however, the declaration stated that the tipper [redacted] (~~TS//STLW//SI//OC/NF~~)

[redacted] was arrested by the FBI later in [redacted] According to the FBI briefing materials, [redacted] (~~S//OC/NF~~)

On [redacted] the FBI applied for and obtained a FISA order to conduct electronic surveillance and a physical search [redacted] By this time, [redacted] had been in FBI custody for several days.[395] In support of the FISA application, the government reported that [redacted] also in custody at that time, recently had [redacted]

[394] Based on the specific wording of the EC, it is evident that the tipper was derived [redacted] (~~TS//STLW//SI//OC/NF~~)

[redacted]

[redacted]

On [redacted] pleaded guilty to [redacted]

[redacted][397] ~~(S//NF)~~

The NSA recommended that the FBI cite [redacted] investigation in briefing materials as an example of Stellar Wind's contribution to counterterrorism efforts. The FBI briefing materials also state that the tipper in [redacted] investigation was "instrumental in [redacted] becoming the subject of a Full Investigation on [redacted]" ~~(TS//STLW//SI//OC/NF)~~

In response to the OIG's request for information about the role [redacted] information played in the investigation [redacted] the FBI's Counterterrorism Division told us [redacted] that, based on its searches of internal FBI databases and discussions with the case agents, "no [redacted] reporting factored into [redacted] investigation." According to a [redacted] declaration the FBI filed in [redacted] prosecution, the [redacted] tipper in [redacted] investigation "did not directly lead to any information or evidence that was used in the prosecution of the case against [redacted] and was not incorporated into any application to a court, including the [FISA Court]."[398] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[398]

[redacted]

~~(TS//STLW//SI//OC/NF)~~

V. OIG Analysis (U)

The FBI created the [redacted] project to disseminate Stellar Wind information as leads to FBI field offices and assigned the CAU's Team 10 to the NSA to work on Stellar Wind full-time for this purpose. We found that the co-location improved the FBI's knowledge about Stellar Wind operations and gave the NSA better insight about how FBI field offices investigated Stellar Wind information. We were told these benefits translated to improvements in the Stellar Wind report drafting process, and by extension, in [redacted] leads. ~~(TS//STLW//SI//OC/NF)~~

One of the changes the FBI implemented to attempt to improve the investigation of [redacted] leads was to make FBI Headquarters-based CAU, instead of the field offices, responsible for issuing National Security Letters (NSL) to obtain subscriber information on tipped telephone numbers and e-mail addresses. This measure, initiated in July 2003, was intended to address agent concerns that [redacted] leads did not provide sufficient information to initiate national security investigations, a prerequisite under Justice Department investigative guidelines to issuing NSLs. ~~(TS//STLW//SI//OC/NF)~~

However, we found that the CAU issued the NSLs from the [redacted] control file, a non-investigative file created in September 2002 to serve as a repository for [redacted]-related communications between FBI Headquarters and field offices. Issuing the NSLs from a control file instead of an investigative file was contrary to internal FBI policy. The FBI finally opened an investigative file for the [redacted] project in November 2006. We believe the CAU and OGC officials involved in the decision to issue NSLs from the [redacted] control file concluded in good faith that the FBI had sufficient predication either to connect the [redacted] NSLs with existing preliminary or full investigations of al Qaeda and affiliated groups or to open new preliminary or full investigations in compliance with Justice Department investigative guidelines. However, we also concluded that the FBI could have, and should have, opened an investigative file for the [redacted] project when the decision first was made to have FBI Headquarters issue NSLs for [redacted] leads. ~~(TS//STLW//SI//OC/NF)~~

We also described in this chapter a change the FISA Court made in March 2004 to the "scrubbing" process used to account for Stellar Wind information in international terrorism FISA applications. The change requires the FBI's Team 10 and FBI OGC, in coordination with the Department's Office of Intelligence (formerly OIPR), to determine whether any facility (telephone number or e-mail address) that appears in a FISA application also appeared in a Stellar Wind report and, if so, whether the FBI had developed, independent of Stellar Wind, an investigative interest in the facility before it was the subject of an [redacted] tipper, or whether the

facility would have been "inevitably discovered." FISA Court Presiding Judge Kollar-Kotelly imposed this additional scrubbing requirement after being advised of modifications made to Stellar Wind in March 2004 following the Justice Department's revised legal analysis of the program. The FBI and Office of Intelligence continue to expend significant resources to comply with this scrubbing requirement.[399] However, we did not find any instances of the requirement causing the FBI not to be able to obtain FISA surveillance coverage on a target. ~~(TS//STLW//SI//OC/NF)~~

Our primary focus in this chapter was to assess the general role of Stellar Wind information in FBI investigations and its value to the FBI's overall counterterrorism efforts. Similar to the FBI, we had difficulty assessing the specific value of the program to the FBI's counterterrorism activities. However, based on our interviews of FBI managers and agents and our review of documents, and taking into account the substantial volume of leads the program generated for the FBI, we concluded that although the information produced under the Stellar Wind program had value in some counterterrorism investigations, it played a limited role in the FBI's overall counterterrorism efforts. ~~(S//NF)~~

The vast majority of Stellar Wind information the NSA provided the FBI related to telephone numbers and e-mail addresses the NSA identified through meta data analysis as having connections to individuals believed to be involved in international terrorism. The NSA rated a small percentage of these contacts [redacted] ~~(TS//STLW//SI//OC/NF)~~

FBI agents and analysts with experience investigating [redacted] leads told us that most leads were determined not to have any connection to

---

[399] As noted earlier, the scrubbing procedure applies both to NSA information derived from the Stellar Wind program and to information derived from the FISA Court's PR/TT and Section 215 bulk meta data orders. This is so because until mid-2008, when the Stellar Wind program officially was closed, leads the NSA developed from the FISA-authorized bulk meta data collections were disseminated under the Stellar Wind compartment. ~~(TS//STLW//SI//OC/NF)~~

[400] Stated another way, the Stellar Wind program generated [redacted] leads for the FBI each month from October 2001 to February 2006. ~~(TS//STLW//SI//OC/NF)~~

terrorism, and they did not identify for us any specific cases where leads helped the FBI identify previously unknown subjects involved in terrorism (although several stated that this did occur). This is not surprising given that the vast majority of leads sent to FBI field offices for investigation concerned telephone numbers and e-mail addresses that the NSA already had determined were at best one or two steps removed from numbers and addresses suspected of being used by individuals believed to be involved in terrorism. (~~TS//STLW//SI//OC/NF~~)

The FBI's two statistical studies that attempted to assess the "significance" of Stellar Wind meta data leads to FBI counterterrorism efforts did not include explicit conclusions on the program's usefulness. The first study found [redacted] samples taken from [redacted] meta data leads the NSA provided the FBI from approximately October 2001 to December 2005, [redacted] or 1.2 percent [redacted] made "significant" contributions. The FBI's second statistical study, which reviewed each [redacted] e-mail tippers the NSA provided the FBI from August 2004 through January 2006, identified no examples of "significant" contributions to FBI counterterrorism efforts.[401] The FBI OGC told us that FBI executive management's statements in congressional testimony that the Stellar Wind program had value was based in part on the results of the first study. (~~TS//STLW//SI//OC/NF~~)

While we believe Stellar Wind's role in FBI cases was limited, assessing the value of the program to the FBI's overall counterterrorism efforts is more complex. Some witnesses commented that an intelligence program's value cannot be assessed by statistical measures alone. Other witnesses, such as General Hayden, said that the value of the program may lie in its ability to help the Intelligence Community determine that the terrorist threat embedded within the country is not as great as once feared. Witnesses also suggested that the value of the program should not depend on documented "success stories," but rather on maintaining an intelligence capability to detect potential terrorist activity in the future. (~~TS//SI//NF~~)

FBI personnel we interviewed generally were supportive of the Stellar Wind (or [redacted] program, calling the information "one tool of many" in the FBI's anti-terrorism efforts that "could help move cases forward" by, for example, confirming a subject's contacts with individuals involved in terrorism or identifying additional terrorist contacts. However, FBI personnel also frequently noted for us the deficiencies in the Stellar Wind information disseminated to FBI field offices, such as the lack of details

[401] As described earlier in this chapter, the FBI considered a tipper "significant" if it led to any of three investigative results: the identification of a terrorist, the deportation from the United States of a suspected terrorist, or the development of an asset that can report about the activities of terrorists. (~~TS//STLW//SI//OC/NF~~)

about the foreign individuals allegedly involved in terrorism with whom domestic telephone numbers and e-mail addresses were in contact. Yet, these FBI employees also believed the possibility that such contacts related to terrorism made investigating the tips worthwhile. Some FBI employees also cited the FBI's increased cooperation with the NSA on international terrorism matters as a side benefit of the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

FBI Director Mueller told us that he believes the Stellar Wind program was useful and that the FBI must follow every lead it receives in order to prevent future terrorist attacks. He said "communications are absolutely essential" to this task and called meta data the "key" to the FBI's communications analysis. Mueller also stated that to the extent such information can be gathered and used legally it must be exploited and that he "would not dismiss the potency of a program based on the percentage of hits." ~~(TS//STLW//SI//OC/NF)~~

We sought to look beyond these comments of general support for Stellar Wind to specific, concrete examples of the program's contributions that also illustrated the role Stellar Wind information could play. We therefore examined five cases frequently cited in documents we reviewed and during our interviews as examples of Stellar Wind's contribution to the FBI's counterterrorism efforts. The cases include [redacted] In another case, Stellar Wind information revealed to the FBI that [redacted] ~~(TS//STLW//SI//OC/NF)~~

In another case [redacted] According to the FBI, while the Stellar Wind information was either never used or "was of no value" in the criminal investigation that led to [redacted] arrest and conviction, it was an [redacted] tipper that led to the national security investigation that preceded the criminal prosecution. ~~(TS//STLW//SI//OC/NF)~~

The final investigation we examined [redacted] did not appear to result directly from Stellar Wind information. The NSA and the FBI at times have cited [redacted] case as an example of the contributions of Stellar Wind to

counterterrorism investigations. An FBI declaration filed in [redacted] prosecution indicated that [redacted] Moreover, the FBI told us in response to our inquiry that Stellar Wind information did not "factor into [redacted] investigation." However, we concluded that Stellar Wind may have played some indirect role [redacted] becoming the subject of a Full Investigation by the FBI. Our review of documents indicated that [redacted] investigation, which appears to have been advanced by Stellar Wind reporting, might have caused the FBI to reopen its investigation [redacted] We were unable to describe with the same certainty as in [redacted] investigation the extent of Stellar Wind's contribution to [redacted] investigation, in part because of differing assessments in the FBI's own documents regarding the role of Stellar Wind this matter. ~~(TS//STLW//SI//OC/NF)~~

In short, we found that Stellar Wind generally has played a limited role in FBI counterterrorism investigations, but that the evidence shows there are cases where Stellar Wind information had value. For example, in some of the cases we examined Stellar Wind information caused the FBI to take action that led to useful investigative results. However, in others the connection between the Stellar Wind information and the FBI's investigative actions was more difficult to discern. ~~(S//NF)~~

As discussed in Chapter Five and in this chapter, Stellar Wind's bulk meta data collection activities were transitioned to FISA authority and are ongoing. The FBI, under the [redacted] project (the successor to [redacted], requires field offices to conduct, at a minimum, threat assessments on telephone numbers and e-mail addresses the NSA derives from this FISA-authorized collection that the FBI is not already aware of, including numbers and addresses one or two steps removed from direct contacts with individuals involved in terrorism. In view of our findings about the Stellar Wind program's contribution to the FBI's counterterrorism efforts, we believe that the FBI should regularly assess the impact [redacted] leads have on FBI field offices and whether limited FBI resources should be used to investigate all of them. ~~(TS//STLW//SI//OC/NF)~~

Another consequence of the Stellar Wind program and the FBI's approach to assigning leads was that many threat assessments were conducted on individuals located in the United States, including U.S. persons, who were determined not to have any nexus to terrorism or

represent a threat to national security.[402] These assessments also caused the FBI to collect and retain a significant amount of personal information about the users of tipped telephone numbers and e-mail addresses. In addition to an individual's name and home address, such information could include where the person worked, records of foreign travel, and the identity of family members. The results of these threat assessments and the information that was collected generally were reported in communications to FBI Headquarters and uploaded into FBI databases.
~~(TS//STLW//SI//OC/NF)~~

The FBI's collection of U.S. person information in this manner is ongoing under the NSA's FISA-authorized bulk meta data collection. To the extent leads derived from this program generate results similar to those under Stellar Wind, the FBI will continue to collect and retain a significant amount of information about individuals in the United States, including U.S. persons, that do not have a nexus to terrorism or represent a threat to national security. ~~(TS//STLW//SI//OC/NF)~~

We recommend that as part of the [redacted] project, the Justice Department's National Security Division (NSD), working with the FBI, should collect information about the quantity of telephone numbers and e-mail addresses disseminated to FBI field offices that are assigned as Action leads and that require offices to conduct threat assessments. The information compiled should include whether individuals identified in threat assessments are U.S. or non-U.S. persons and whether the threat assessments led to the opening of preliminary or full national security investigations. With respect to threat assessments that conclude that users of tipped telephone numbers or e-mail addresses are not involved in terrorism and are not threats to national security, the Justice Department should take steps to track the quantity and nature of the U.S. person information collected and how the FBI retains and utilizes this information. This will enable the Justice Department and entities with oversight responsibilities, including the OIG and congressional committees, to assess the impact this intelligence program has on the privacy interests of U.S. persons and to consider whether, and for how long, such information should be retained. ~~(TS//SI//OC/NF)~~

[402] [redacted]

We also recommend that, consistent with NSD's current oversight activities and as part of its periodic reviews of national security investigations at FBI Headquarters and field offices, NSD should review a representative sampling [redacted] leads to those offices. For each lead examined, NSD should assess FBI compliance with applicable legal requirements in the use of the lead and in any ensuing investigations, particularly with the requirements governing the collection and use of U.S. person information. ~~(TS//SI//OC/NF)~~

In sum, we agree that it is difficult to assess or quantify the effectiveness of a particular intelligence program. However, based on the interviews we conducted and documents we reviewed, we found that Stellar Wind information generally played a limited role in the FBI's counterterrorism efforts, but that the information had value in some cases. In addition, some witnesses said the program provides an "early warning system" to allow the Intelligence Community to detect potential terrorist attacks, even if the system has not specifically uncovered evidence of preparations for such an attack. Moreover, other OIGs in the Intelligence Community are reviewing their agency's involvement with the program and the results of those reviews, analyzed together, will provide a more comprehensive picture of the program's overall usefulness. ~~(TS//STLW//SI//OC/NF)~~

Finally, because the bulk meta data aspect of the Stellar Wind program continues under FISA authority, we recommend that the NSD take steps to gather information on the continuing operations of the program, including the use and handling of vast amounts of information on U.S. persons and the effectiveness of the program in FBI counterterrorism investigations. ~~(TS//STLW//SI//OC/NF)~~

CHAPTER SEVEN
DISCOVERY ISSUES RELATED TO STELLAR WIND INFORMATION ~~(TS//SI//NF)~~

In this chapter we discuss the government's statutory and judicial discovery obligations in international terrorism cases relating to Stellar Wind-derived information. Under the Stellar Wind program, the federal government collected vast amounts of information, including the content of communications and meta data about telephone and e-mail communications involving U.S. citizens and non-U.S. citizens. [redacted] potentially triggering an obligation under the Federal Rules of Criminal Procedure and applicable case law for the government to disclose certain information to the defendant. This obligation created a tension between the need to protect the secrecy of the Stellar Wind program and the need to comply with legal disclosure requirements. ~~(TS//STLW//SI//OC/NF)~~

In this chapter, we examine the process by which the Department of Justice attempted to resolve this tension and meet its discovery obligations to criminal defendants.[403] (U)

I. Relevant Law (U)

The government's obligation to disclose certain statements made by a defendant and to disclose other information concerning a defendant in a criminal proceeding comes primarily from two sources: Federal Rule of Criminal Procedure 16 and the U.S. Supreme Court case of *Brady v. Maryland*, 373 U.S. 83 (1963). (U)

Federal Rule of Criminal Procedure 16(a)(1)(B)(i) requires the government to make various disclosures at the request of a criminal defendant. Among other things, the government must disclose "any relevant written or recorded statement by the defendant if the statement is within the government's possession, custody, or control; and the attorney for the government knows – or through due diligence could know – that the statement exists[.]" Rule 16(a)(1)(E) provides that, upon a defendant's request, the government must allow a defendant to inspect and copy papers,

[403] In our review, we did not seek to determine what the government disclosed in specific cases. Rather, we focused on the adequacy of the process that the Justice Department implemented to comply with its discovery obligations in cases that involved Stellar Wind-derived information. ~~(TS//STLW//SI//OC/NF)~~

documents, data, and other materials "if the item is within the government's possession, custody, or control" and the item is material to preparing the defense; the government intends to use the item in its case-in-chief at trial; or the item was obtained from or belongs to the defendant. (U)

Under Rule 16, a defendant's statements carry a "near presumption of relevance," and "the production of a defendant's statements has become 'practically a matter of right even without a showing of materiality.'" *United States v. Yunis*, 867 F.2d 617, 621-22, 625 & n.10 (D.C. Circuit 1989).[404] (U)

Disclosure of a defendant's statements is usually made by the government after receiving a request pursuant to Rule 16. However, even without making a Rule 16 request, a defendant has an independent right to discovery of his statements and certain other relevant information under *Brady v. Maryland*, 373 U.S. 83 (1963). *Brady* requires the government to disclose evidence in its possession favorable to the defendant and material to either guilt or punishment. Material evidence must be disclosed if it is exculpatory or if it could be used to impeach a government witness. (U)

According to an Office of Intelligence Policy and Review (OIPR) memorandum on the government's Rule 16 and *Brady* obligations [redacted][405] (U)

However, according to the memorandum, when production of the defendant's statements or other information would reveal classified information, the government may assert a national security privilege, sometimes known as the state secrets privilege.[406] If the government asserts a colorable claim in a legal proceeding that classified information is privileged, the defendant must show that the information is not only

---

[404] See also *United States v. Scarpa*, 913 F.2d 993, 1011 (2nd Cir. 1990), citing *United States v. McElroy*, 697 F.2d 459, 464 (2nd Cir. 1982)("Rule 16 does not cover oral statements unrelated to the crime charged or completely separate from the government's trial evidence."). (U)

[405] Counsel for Intelligence Policy James Baker told us the memorandum was drafted at his request by an Assistant U.S. Attorney who had been detailed to OIPR. Baker said he requested the memorandum to refresh his understanding of the government's discovery obligations in criminal prosecutions. (U//~~FOUO~~)

[406] The state secrets privilege is a common law doctrine asserted by the United States government to protect classified information. See generally, *United States v. Reynolds*, 345 U.S. 1 (1952). (U)

relevant but material. If the defendant can show materiality, some courts balance the defendant's need for disclosure against the government's substantial interest in protecting sources and methods associated with the sensitive information. See *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988); *United States v. Smith*, 781 F.2d 1102, 1180 (4th Cir. 1985) (en banc). (U)

The government can also invoke the Classified Information Procedures Act (CIPA), 18 U.S.C. App. 3, to protect classified information in federal prosecutions. CIPA does not expand or limit a defendant's right to discovery under Rule 16; rather, CIPA allows a court, "upon a sufficient showing" to authorize the government to delete specified items of classified information from otherwise discoverable documents, substitute a summary of the information, or stipulate to relevant facts that the classified information would tend to prove. (U)

As detailed below, after aspects of the Stellar Wind program were disclosed in The New York Times and confirmed by the President in December 2005, the Justice Department invoked CIPA to prevent disclosure of the program and any program-derived information in [redacted] criminal cases, [redacted] ~~(TS//STLW//SI//OC/NF)~~

II. Cases Raise Questions about Government's Compliance with Discovery Obligations (U)

The tension between the highly classified nature of the Stellar Wind program and the government's discovery obligations in criminal cases initially arose in [redacted] ~~(TS//STLW//SI//OC/NF)~~

A. [redacted] (TS//STLW//SI//OC/NF)

The Department's awareness that Stellar Wind would have [redacted] implications in criminal discovery arose in a case involving [redacted]

[redacted]

[redacted]

(Cont'd.)

information collected under Stellar Wind would be discoverable and, more generally, how the Stellar Wind collections might be treated in view of the government's discovery obligations in criminal prosecutions. ~~(TS//STLW//SI//OC/NF)~~

Baker said he raised these issues with Attorney General Ashcroft, FBI Director Mueller, and other Justice Department, FBI, and NSA officials. Baker stated that they concluded that a determination should first be made whether the [redacted] obtained through Stellar Wind also were captured through FISA and therefore could be produced. Baker said it turned out [redacted] had been intercepted under FISA and could be produced under that authority rather than as a result of Stellar Wind collections. Baker told the OIG that he was relieved by this outcome, but continued to be concerned about future cases. ~~(TS//STLW//SI//OC/NF)~~

B. [redacted] (TS//STLW//SI//OC/NF)

[redacted]

[redacted]

~~(TS//STLW//SI//OC/NF)~~

[redacted]

On [redacted] Yoo orally recommended to Ashcroft that the Justice Department not disclose the Stellar Wind program intercepts to the [redacted] Yoo subsequently memorialized his advice in a memorandum. ~~(TS//STLW//SI//OC/NF)~~

[redacted]

[redacted]

Yoo finished his written memorandum regarding [redacted]

[redacted]

[redacted]

[

[redacted][411]
~~(TS//STLW//SI//OC/NF)~~

[redacted]
~~(TS//STLW//SI//OC/NF)~~

As a final point, Yoo wrote, [redacted]
~~(TS//STLW//SI//OC/NF)~~

[redacted]

411 [redacted]

412 At the time Yoo wrote the [redacted] memorandum, he, Baker, and Ashcroft were the only non-FBI Justice Department officials read into the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

413 [redacted]

414 [redacted]

(Cont'd.)

[redacted]

In another internal Justice Department review of his actions, Yoo has acknowledged that he is not well versed in criminal law. During an interview with the Department's Office of Professional Responsibility (OPR) in connection with its investigation concerning his legal opinions in support of a detainee interrogation program, Yoo stated that "criminal prosecution process in the Department was not my specialty," and "criminal law was not my area."[415] ~~(TS//SI//OC/NF)~~

III. Criminal Division Examines Discovery Issues (U)

Following [redacted] the Justice Department's Criminal Division was tasked with developing procedures for handling Rule 16 disclosure issues because the issues fell within its area of expertise. As a result, in [redacted] Patrick Rowan, a senior counsel in the Criminal Division, was read into the program to deal with Stellar Wind-related discovery issues. Rowan's supervisor, Criminal Division Assistant Attorney General Christopher Wray, was also read into the program at the same time.

[redacted]

[415] The OPR investigation concerned a Top Secret compartmented program relating to detainee interrogations. Yoo drafted legal opinions for this program while in the Office of Legal Counsel. However, as discussed in Chapter Four, in contrast with the Stellar Wind program at least four other OLC attorneys assisted Yoo with drafting the legal memoranda. Yoo was also able to consult with Criminal Division attorneys and the client agency on this matter. ~~(TS//STLW//SI//OC/NF)~~

Wray and Rowan were the first Department attorneys with Criminal Division-level responsibility for terrorism prosecutions to be read into the program. ~~(TS//STLW//SI//OC/NF)~~

Wray told the OIG that after his and Rowan's read-in, they "were kind of left on our own." He said that no one directed him or Rowan to continue studying the Rule 16 issues or the government's *Brady* obligations in connection with international terrorism prosecutions, nor did anyone tell them to develop any judgments or opinions on the subject. (U)

Wray told us that at some point after his read-in he may have read Yoo's [redacted] memorandum on the Department's discovery obligations in [redacted] and he instructed Rowan to review the memorandum. Rowan told us that he was familiar with Yoo's memorandum, but stated that he could not recall whether the purpose of Yoo's memorandum was to lay out in general the pertinent legal issues or to document how [redacted] in particular was to be handled. Rowan told us that he did not recall having any problems with the conclusions Yoo reached. ~~(TS//STLW//SI//OC/NF)~~

A. The "Informal Process" for Treating Discovery Issues in International Terrorism Cases (U)

During his OIG interview, Rowan described the processes at the Department prior to the December 2005 disclosure of aspects of the Stellar Wind program in The New York Times to address discovery obligations with respect to Stellar Wind-derived information. He said that the NSA was generally aware of the Justice Department's international terrorism criminal cases, at least in part due to NSA's ongoing contacts with Patrick Philbin and others in the Department. According to Rowan, the NSA's general awareness of the Department's international terrorism docket amounted to an "informal process" for spotting cases that may present discovery issues. Rowan stated that prosecutors in U.S. Attorney's Offices typically would request the NSA to perform "prudential searches" of its databases for any relevant information concerning their prosecutions, including for discovery purposes, although this did not happen in every international terrorism case. Rowan stated that if the NSA located any responsive but classified information, it would be expected to notify senior Justice Department officials with the requisite clearances about the information. Rowan said he was confident that if *Brady* information were known to the NSA, it would be brought to the attention of the Department and steps would have been taken to dismiss the case or otherwise ensure the program was not disclosed. ~~(TS//STLW//SI//OC/NF)~~

In addition to these routine communications between Department prosecutors and the NSA in criminal prosecutions, Rowan described other

measures that were in place to keep Stellar Wind-derived information out of the criminal prosecution process. He stated that the FBI had "walled off" any evidence it collected from inclusion in criminal cases by tipping out Stellar Wind-derived information under [redacted] with a caveat that the information in the tipper was "for lead purposes only." Rowan noted that OIPR also had in place a scrubbing process to delete program-derived information from FISA applications. Rowan expressed confidence that these mechanisms ensured that no program information was used in international terrorism prosecutions.[416] Finally, Rowan stated that the FBI is "very quick to get FISAs up," thereby minimizing the likelihood that the NSA's Stellar Wind database would be the sole repository of *Brady* material. ~~(TS//STLW//SI//OC/NF)~~

B. [redacted] Memorandum Analyzing Discovery Issues Raised by the Stellar Wind Program ~~(TS//STLW//SI//OC/NF)~~

At the direction of Assistant Attorney General Wray, Rowan memorialized his research regarding these discovery issues in a memorandum entitled [redacted] Rowan said he worked on the memorandum largely alone, consulting occasionally with Wray. Rowan said it was very difficult to work on the matter because of the secrecy surrounding the program and the other demands of his job.[417] ~~(TS//STLW//SI//OC/NF)~~

In his [redacted] memorandum, [redacted]

[416] As discussed in Chapter Six, the caveats were intended to exclude at the outset any Stellar Wind-derived information from FISA applications and other criminal pleadings. The scrubbing process acts as a second check against including this information in FISA applications. However, neither the caveats nor the scrubbing process relieved the government of its obligations under *Brady* to disclose evidence in the government's possession favorable to the defendant and material to either guilt or punishment. ~~(TS//STLW//SI//OC/NF)~~

[417] The memorandum noted, "Because there were no additional attorneys within the Criminal Division who were read into the program (and very few in the Department generally), we have been unable to assign work to others or to fully consult with others within the Division." ~~(TS//SI//NF)~~

[redacted]

[redacted]

Rowan's memorandum also referred to guidance in the United States Attorney's Manual (USAM). For cases in which the Intelligence Community had no active involvement in the criminal investigation, the USAM stated that there are two circumstances in which the prosecutor must conduct a "suitable search" of Intelligence Community files: (1) where the prosecutor has "direct or reliable knowledge" that the Intelligence Community

[redacted]

possesses potential *Brady* or other discovery material; or, (2) in the absence of such knowledge, where "there nonetheless exists any reliable indication suggesting" that the Intelligence Community possesses such material. USAM, Criminal Resources Manual § 2052 (2002). The USAM stated that, as a general rule, a prosecutor should not seek access to Intelligence Community files unless there is an affirmative obligation to do so. However, it noted that certain types of cases, including terrorism prosecutions, fall outside this general rule. In such cases, the USAM advised that the prosecutor should conduct a "prudential search." Id. ~~(TS//STLW//SI//OC/NF)~~

Rowan wrote that the practice in several sections within the Criminal Division was to "generally go beyond both the legal obligations outlined [in his memorandum] and the general rule outlined in the USAM, initiating searches out of prudence, rather than a legal obligation." For instance, Rowan reported that the practice of the Criminal Division's Counterespionage Section (CES) was to search Intelligence Community files in almost every case, even in instances in which the Intelligence Community had no involvement in the investigation or prosecution [redacted].[420] ~~(TS//STLW//SI//OC/NF)~~

[redacted][421] In cases involving the NSA, the typical practice

---

[420] The OIG interviewed John Dion, the Chief of CES, which became part of the National Security Division in 2006. [redacted] Dion stated that such searches are conducted in cases in which there is likely to be intelligence collection concerning the defendant as "suggested by the facts of the matter." He added that the searches were requested for a variety of reasons, including for purposes of meeting discovery obligations. Dion said that searches also were requested to determine whether the defendant has a "relationship" with an intelligence agency. He noted that CES does not request prudential searches as a matter of course to avoid making spurious requests. ~~(S//NF)~~

[421] [redacted] Dion said CES was a proponent of the position that line prosecutors with whom CES co-prosecutes cases should have the same knowledge as CES concerning the "national security equities" involved in each case. Dion said this arrangement also allows for the AUSA, who is often the prosecutor most familiar with the case and the jurisdictional practices, to review any Intelligence Community material for Rule 16 and *Brady* purposes. Dion acknowledged the limitations to this arrangement concerning strictly compartmented programs such as Stellar Wind, where the NSA understandably would be reluctant to read in line prosecutors for the limited purpose of screening defense discovery requests. ~~(TS//STLW//SI//OC/NF)~~

was for the CES attorney to use the provisions of CIPA to prevent disclosure of sensitive material. Rowan noted that other sections within the Criminal Division also relied on CIPA to protect Intelligence Community files found during searches. ~~(TS//SI//OC/NF)~~

[redacted]

[redacted]

Thus, although Rowan's memorandum did not contain a proposal for handling discovery requests in cases involving Stellar Wind, it identified key legal issues that would have to be addressed as a part of any such proposal.

[redacted]

~~(TS//STLW//SI//OC/NF)~~

---

[422] When Rowan became principally responsible for coordinating the Department's responses to defense discovery requests as a Deputy Assistant Attorney General in the (Cont'd.)

C. Office of Legal Counsel and Discovery Issue (U)

Shortly before Rowan finished his memorandum in [redacted] OLC Principal Deputy Assistant Attorney General Steve Bradbury became the acting head of OLC. Bradbury told us that he recalled having some discussion with Rowan about how discovery matters should be handled in connection with the Stellar Wind program. Bradbury said that John Eisenberg, later a Deputy in OLC, also may have discussed the matter with Rowan. Bradbury stated that he did not believe that OLC followed up on Rowan's request that it continue researching these issues. ~~(TS//STLW//SI//OC/NF)~~

Eisenberg told us that he discussed the Rule 16 issue with Rowan at some point, but did not recall whether they discussed the *Brady* issue. He recalled discussing Yoo's [redacted] memorandum with Rowan and said he believes the Justice Department took the position that the Yoo memorandum was correct, at least with respect to Yoo's legal analysis in [redacted] ~~(TS//STLW//SI//OC/NF)~~

When we showed Eisenberg a copy of Rowan's [redacted] memorandum, Eisenberg stated that he had not previously seen it. Eisenberg told us that OLC would not typically be responsible for addressing the discovery issues presented in Rowan's memorandum and that he was not aware of any OLC opinion on the subject other than Yoo's memorandum. Eisenberg also said he was not aware of any formal procedures for handling Rule 16 disclosure requests or the government's affirmative *Brady* obligations other than the *ex parte* in camera motions practice pursued by the National Security Division, discussed below. ~~(TS//STLW//SI//OC/NF)~~

CES Chief Dion agreed that OLC would not be the appropriate entity to review discovery procedures in the context of Stellar Wind, in part because OLC attorneys generally do not have criminal litigation expertise. Dion suggested that if the Department were to develop procedures for handling discovery of Intelligence Community files, it should be done by the Department's National Security Division in coordination with United States Attorneys' Offices, and it should be binding only on those two entities. Rowan, while generally agreeing with Dion, told the OIG that he believed the OLC appropriately could have analyzed the legal issue of what impact a

---

National Security Division in 2006. [redacted] The results of these searches were produced to the courts *ex parte*, in camera, pursuant to CIPA. ~~(TS//STLW//SI//OC/NF)~~

guilty plea would have on the government's *Brady* obligations. ~~(TS//STLW//SI//OC/NF)~~

[redacted]

IV. Use of the Classified Information Procedures Act (CIPA) to Respond to Discovery Requests (U)

After publication of The New York Times articles in December 2005, the Justice Department received numerous discovery requests in connection with international terrorism prosecutions throughout the country. After these articles, additional officials in the Criminal Division were read into the Stellar Wind program, including the new Assistant Attorney General Alice Fisher and other senior officials, both to assist with the Criminal Division's investigation into the leak of information to The New York Times and to handle the discovery requests following the public confirmation of the program by the President and other Administration officials in December 2005.[423] After the National Security Division was created in September 2006, it assumed much of the responsibility for handling the responses to discovery requests. ~~(TS//STLW//SI//OC/NF)~~

Typically, the defense motions sought to compel the government to produce information concerning a defendant that had been derived from the "Terrorist Surveillance Program," the term sometimes used by the government to refer to what the President confirmed after publication of The New York Times articles. The government responded to the discovery requests by filing *ex parte* in camera responses requesting to "delete items" from material to be produced in discovery pursuant to CIPA. ~~(S//NF)~~

In the following sections we provide a brief overview of CIPA and its use in international terrorism cases potentially involving Stellar Wind-derived intelligence. ~~(TS//STLW//SI//OC/NF)~~

[423] [redacted]

A. Overview of CIPA (U)

The Classified Information Procedures Act, 18 U.S.C. App. 3, was enacted in 1980 to provide procedures for protecting classified information in federal criminal prosecutions. When a party to a criminal proceeding notifies the court that classified information will be used in the course of the proceeding, CIPA requires the court to initiate procedures to "determine the use, relevance, or admissibility of the classified information that would otherwise be made during the trial or pretrial proceeding." 18 U.S.C. App. 3 § 6(a). Where the government holds the classified information, it may bring the matter before the court *ex parte*, but it also must provide notice to the defense that classified information is at issue. Id. at § 6(b)(1). (U)

Protective procedures generally are established through a CIPA hearing with both parties present. The hearing may be conducted in camera if the government certifies that an in camera hearing is necessary to protect the classified information. Id. at § 6(a). Typically, the government seeks an order to protect against the disclosure of any classified information to the defense. The government may also seek to withhold production of the classified information in one of three ways: (1) deletion of the classified items from the material disclosed to the defendant, (2) summarization of the classified information, or (3) admission of certain facts that the classified information would tend to prove. Id. at § 4. Based on the OIG's review of CIPA filings related to the Stellar Wind program, the government has only used option 1 (deleting classified items from material to be disclosed to the defendant) in response to defense motions for Stellar Wind information. ~~(TS//STLW//SI//OC/NF)~~

To prevent the disclosure of classified information, the government may make an *ex parte* showing to the court. To do so the government must submit "an affidavit of the Attorney General certifying that disclosure of classified information would cause identifiable damage to the national security of the United States and explaining the basis for the classification of such information." Id. at § 6(c)(2). If the court decides that the defendant's right to access to the evidence outweighs the government's national security interests, the government can choose to dismiss the indictment rather than make a disclosure. *United States v. Moussaoui*, 382 F.3d 453, 466 n. 18, 474-76 (4th Cir. 2004). (U)

B. Use of CIPA in International Terrorism Prosecutions Alleged to Involve Stellar Wind-Derived Information ~~(TS//STLW//SI//OC/NF)~~

We reviewed the CIPA pleadings files maintained in the National Security Division relating to the Stellar Wind program. In almost every instance, the CIPA litigation was handled by the National Security Division

without the involvement of the line prosecutors in the U.S. Attorney's Offices who handled the underlying prosecutions but who were not read into the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

[redacted] Rowan, who became the National Security Division Acting Assistant Attorney General in April 2008 and was confirmed as the Assistant Attorney General in September 2008, told us that [redacted] ~~(TS//STLW//SI//OC/NF)~~

The scope and nature of the defense motions initiating the CIPA litigation varied, depending on the procedural posture of the case. For instance, some defense motions sought to compel discovery of NSA surveillance information, while others sought to suppress all government evidence and, in the alternative, have the government's case dismissed on the theory that illegal electronic surveillance caused the government to initiate its criminal investigation in the first instance. [redacted] ~~(TS//STLW//SI//OC/NF)~~

Regardless of the varying procedural posture of the cases and the scope and nature of the defense motions, the government responses we examined were fairly uniform, consisting of a motion to delete items from discovery, a legal memorandum in support of the motion, declarations from senior FBI and NSA officials, and a proposed order. ~~(TS//STLW//SI//OC/NF)~~

[redacted] ~~(TS//STLW//SI//OC/NF)~~

The government's CIPA submissions asserted that the information at issue in the discovery litigation was classified and subject to the national security privilege as codified in CIPA. They generally described the types of information its searches of intelligence databases (including Stellar Wind) might reveal. [redacted]

[redacted]

424 [redacted]

[redacted][425]

The government's responses we reviewed uniformly stated that information in the NSA's intelligence reports had not been or would not be used as evidence, and that there was no causal connection between the information in the reports and any evidence used or to be used at trial, or was too attenuated from the evidence to be discoverable. The government argued that because the facts concerning the NSA's reporting would not aid the defense, the court need not explore the sources and methods used to acquire the information. The submissions also argued that the information collected by the NSA was not included in the government's FISA application, and therefore was too attenuated from the trial evidence to merit a review of the means by which the intelligence information was gathered. The government asserted that the "causal connection" between discovery of the derivative evidence and the alleged illegal search "may have become so attenuated as to dissipate the taint."[426] It is important to note that the government did not argue in the CIPA responses we reviewed that [redacted] (~~TS//STLW//SI//OC/NF~~)

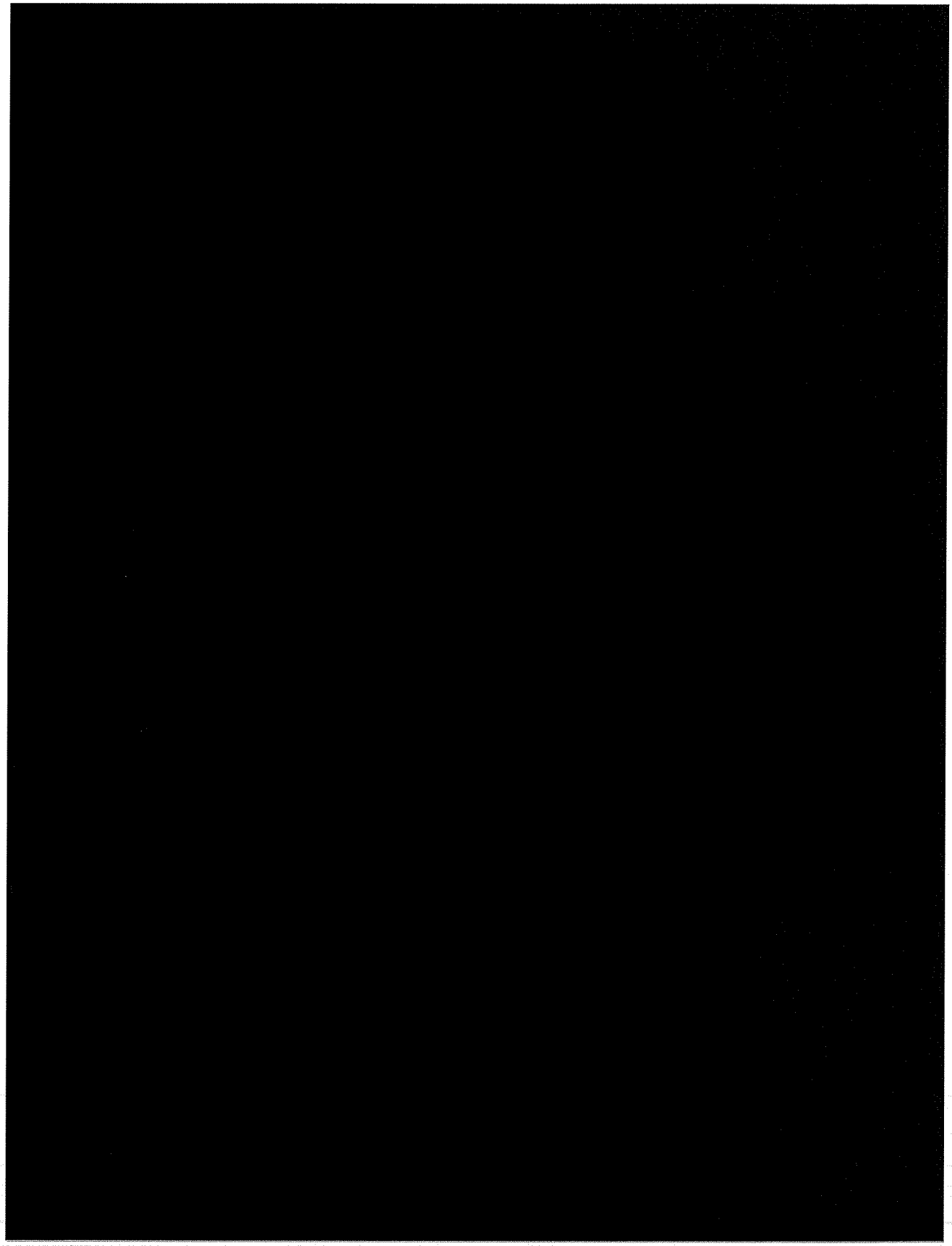
C. Government Arguments in Specific Cases (U)

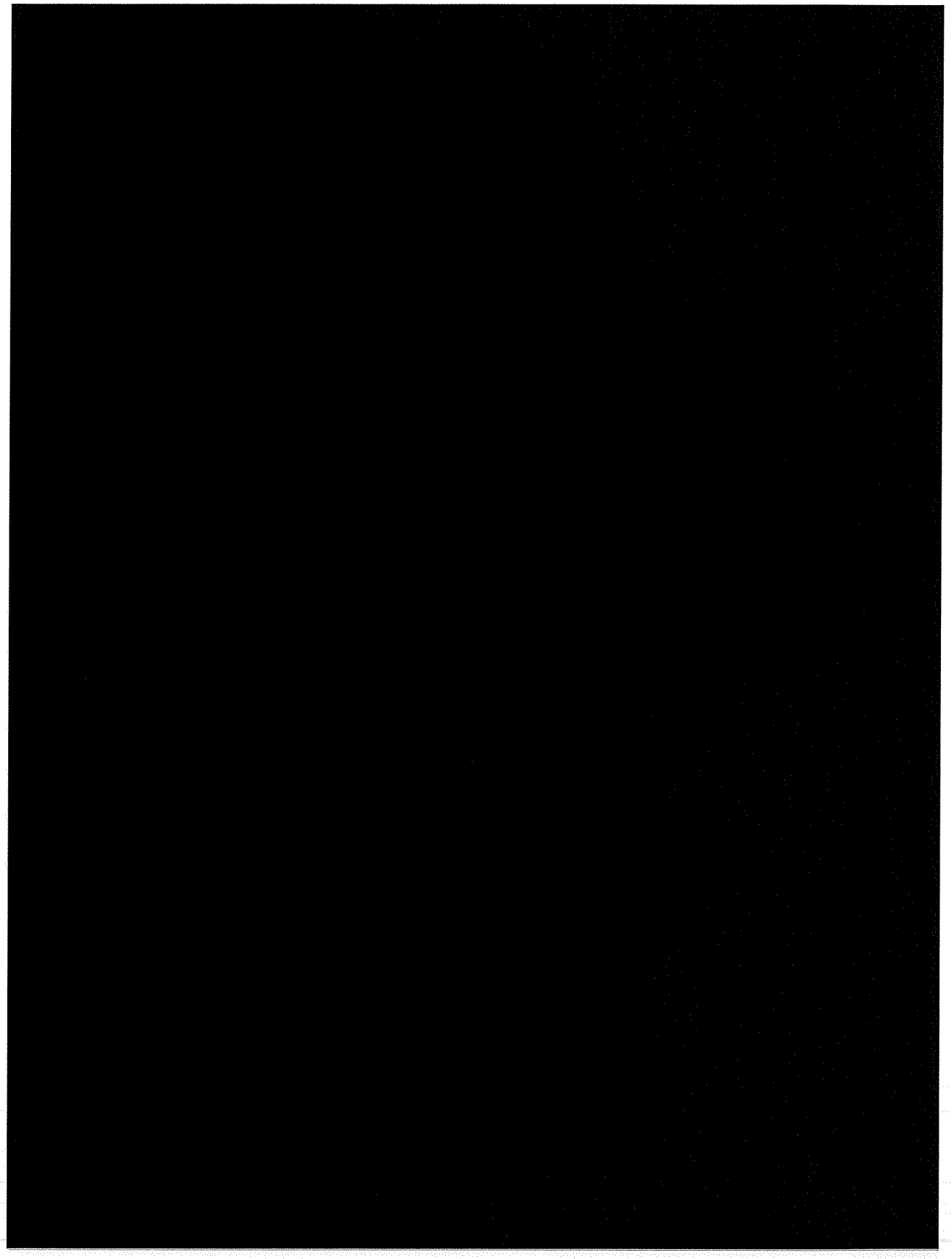
In this section we describe [redacted] cases that illustrate the arguments made by the government in CIPA litigation with respect to defendant's requests for discovery of Stellar Wind-derived information. ~~(TS//STLW//SI//OC/NF)~~

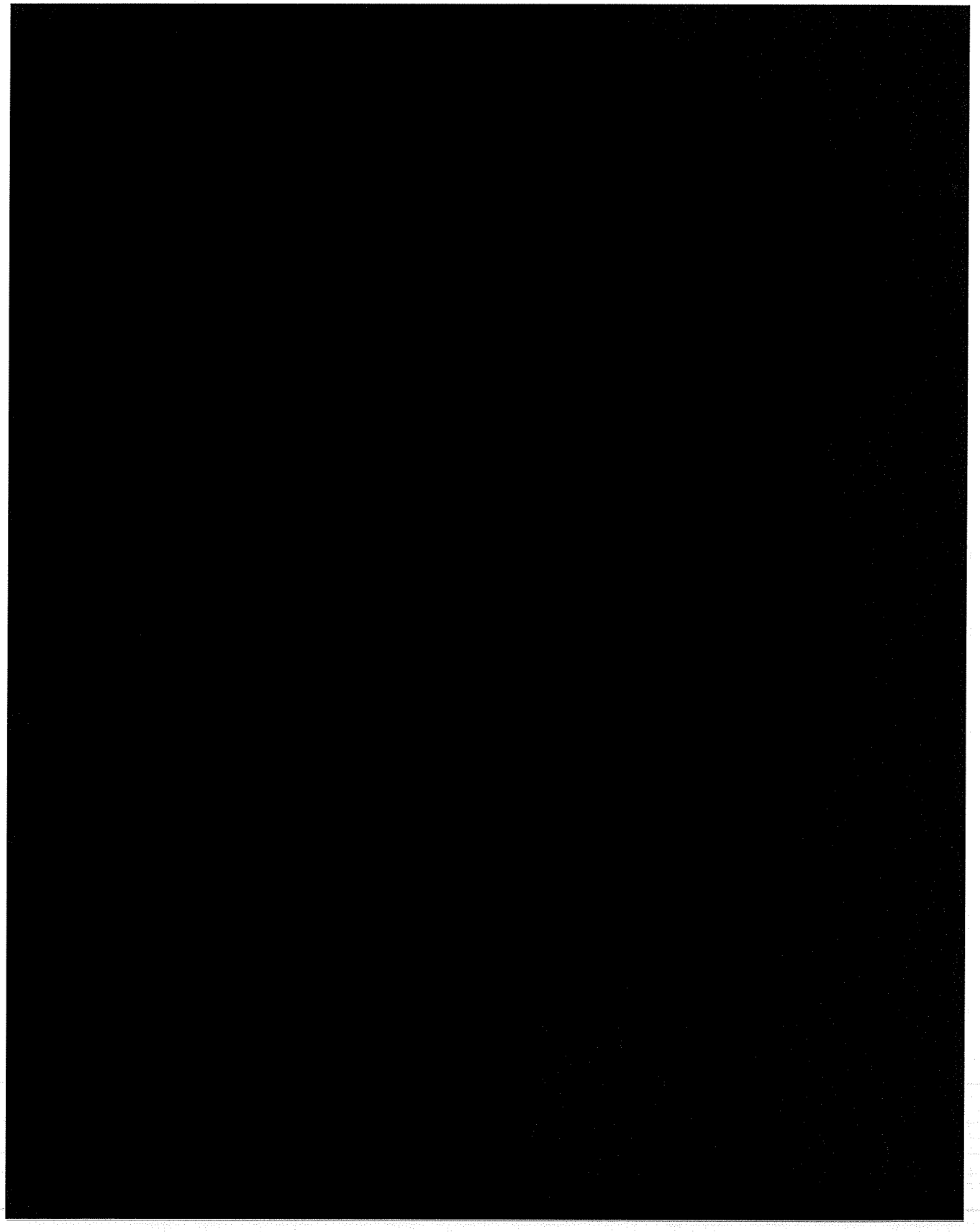
[redacted]

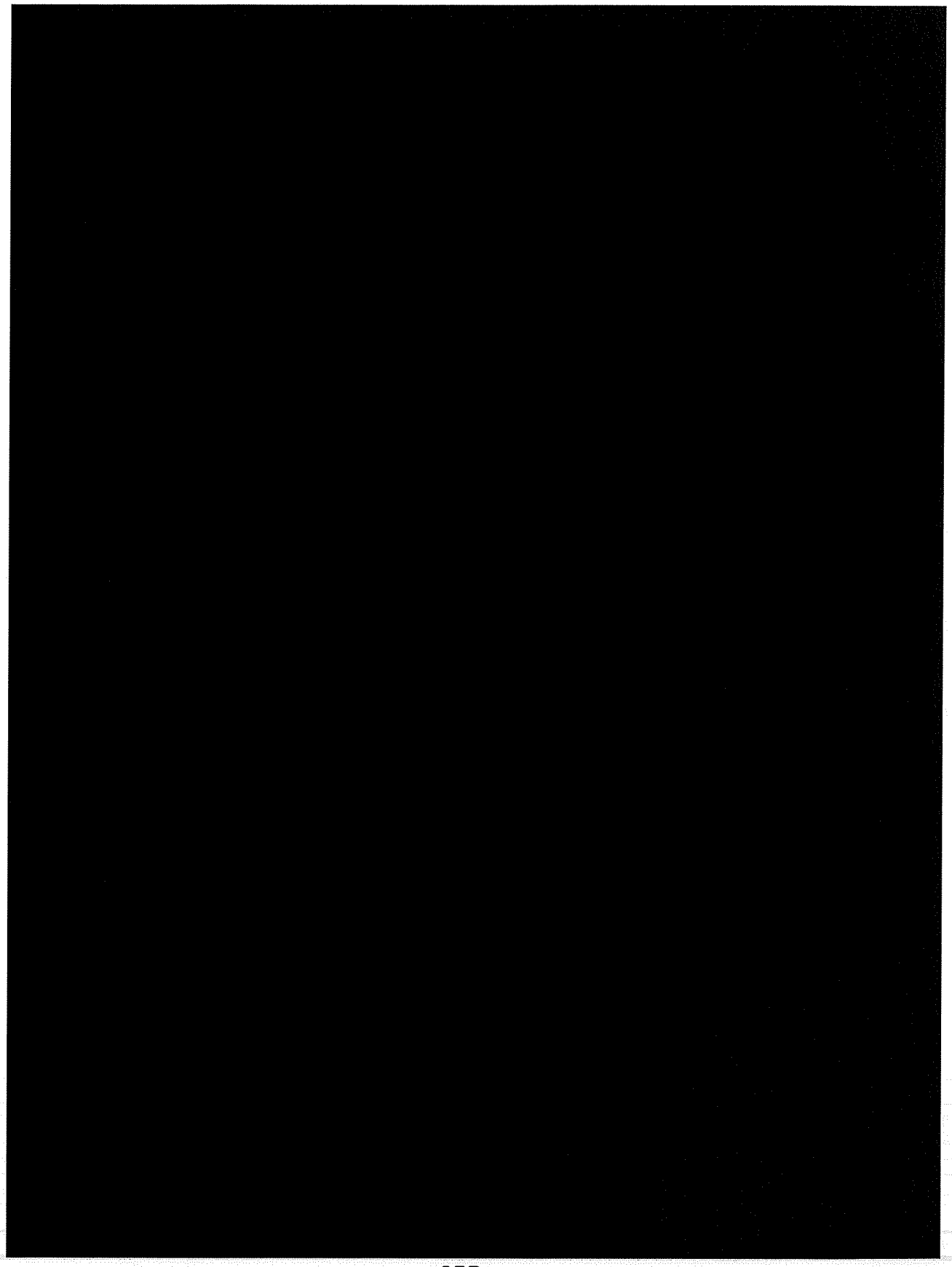
[425] In several instances, the Stellar Wind information was disseminated within the FBI after the FBI already had obtained a FISA order to conduct electronic surveillance of the defendant, thus allowing the government to argue that the NSA reporting played no role in its acquisition of the evidence used or planned to be used against the defendant. ~~(TS//STLW//SI//OC/NF)~~

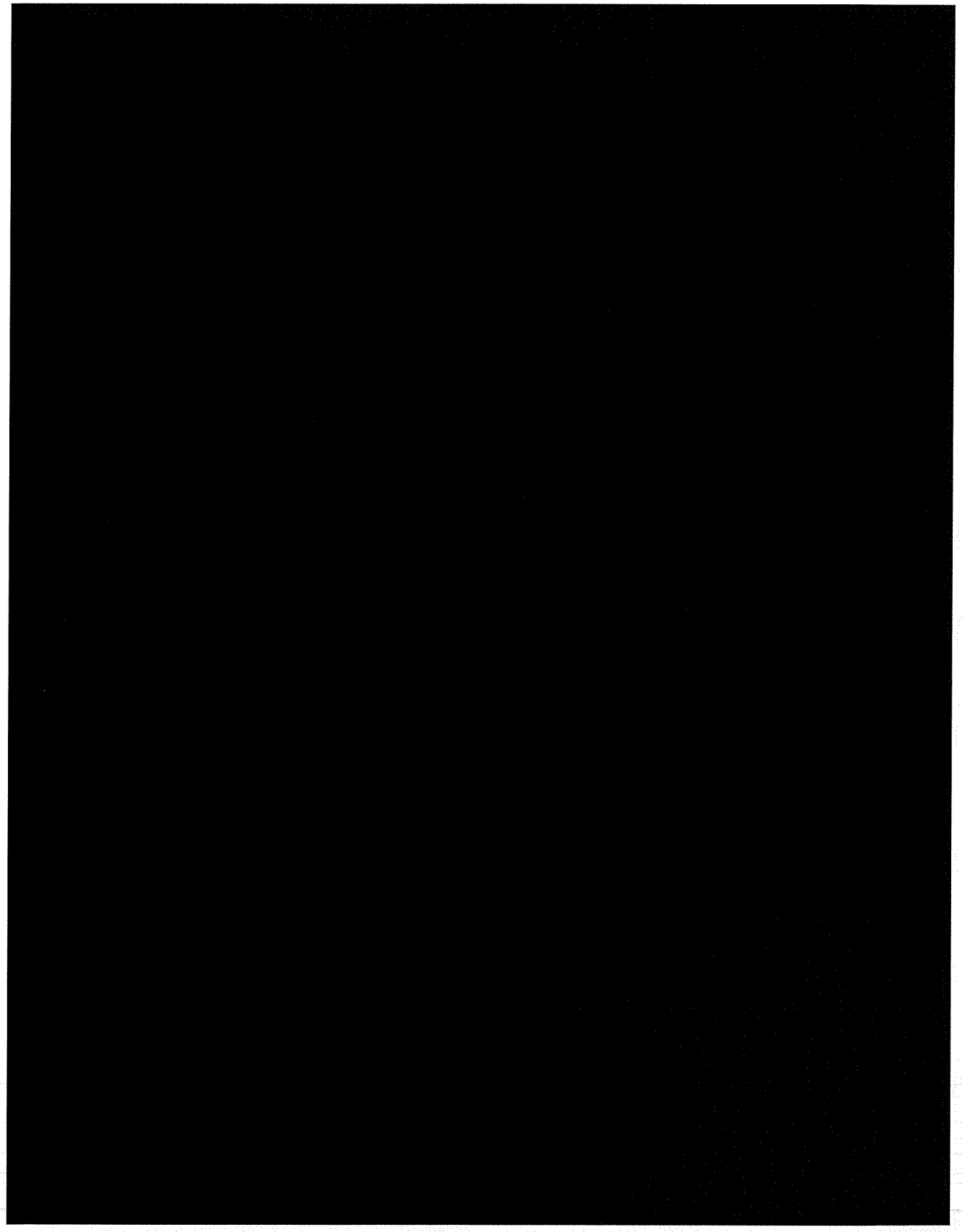
[426] *Nardone v. United States*, 308 U.S. 338, 341 (1939). The government also argued in its submissions that suppressing its evidence would not serve any deterrence purpose. The government argued that the NSA acquires, processes, and disseminates intelligence not to produce criminal prosecutions, but to protect the national security. It asserted that any suppression of evidence would therefore frustrate a criminal prosecution and create an incentive for the intelligence community not to share information with law enforcement, thereby harming national security. ~~(TS//SI//OC/NF)~~











[redacted]

V. OIG ANALYSIS (U)

We found that the Department made little effort to understand and comply with its discovery obligations in connection with Stellar Wind-derived information for the first several years of the program. The Department's limited initial effort was also hampered by the limited number of attorneys who were read into the program. As a result, OLC attorney John Yoo alone initially analyzed the government's discovery obligations in one early case, and he produced a legal analysis that was based on an incorrect understanding of the facts of the case to which it applied. When other attorneys from the Department's Criminal Division eventually were read into the program, [redacted] At that point, the Department eventually took steps to address [redacted] its discovery obligations. However, in our view, those steps are not complete and do not fully ensure that the government has met its discovery obligations regarding information obtained through the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

As described in this chapter, in 2002 the Department first recognized that the Stellar Wind program could have implications for discovery obligations in terrorism cases. OIPR Counsel Baker raised with Department

[redacted]

and FBI officials the question of how the government would meet its discovery obligations regarding Stellar Wind information. Despite awareness of this issue, the Department took no action at this time to ensure that it was in compliance with Rule 16 or *Brady* with respect to Stellar Wind-derived information. We believe that at this point senior Department officials were on notice that, at a minimum, the discovery issue merited attention. However, no concrete action was taken until early [redacted] in the context of [redacted] when the Department had to address how to handle Stellar Wind information that was not also obtained under FISA and that could be material to the defense under Rule 16. This issue was assigned to Yoo, who concluded [redacted]

[redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

As with other aspects of the Stellar Wind program, we believe the error in Yoo's legal analysis may have resulted in part from the failure to subject his memorandum to typical OLC and Department review and scrutiny. Because other Department attorneys were not read into the Stellar Wind program, the risk that the Department would produce a factually flawed and inadequate legal analysis of these important discovery issues was escalated. As we concluded in Chapters Three and Four, we believe the lack of sufficient legal resources at the Department during this early phase of the Stellar Wind program hampered its legal analysis of important issues related to the program. We believe that Yoo's [redacted] memorandum is one more manifestation of this problem. ~~(TS//STLW//SI//OC/NF)~~

In July 2004, Patrick Rowan, a senior counsel in the Criminal Division, was read into the program and conducted a more systemic analysis of the Department's discovery obligations with regard to Stellar Wind information. [redacted]

[redacted]

[redacted] ~~(TS//STLW//SI//OC/NF)~~

[redacted]

With his memorandum, Rowan initiated a request that the issue be further examined by OLC. ~~(TS//SI//NF)~~

However, other than in informal discussions with Rowan concerning Yoo's [redacted] memorandum, OLC did not further examine these issues or follow up on Rowan's recommendation. While we recognize that OLC was not responsible for developing litigative strategy on this issue, we believe that OLC or another appropriate Department component should have provided guidance on this important legal issue. ~~(TS//STLW//SI//OC/NF)~~

We recommend that the Department conduct a comprehensive legal assessment of the important issues [redacted] that still remain unresolved [redacted] the legal ramifications of a guilty plea on the government's disclosure obligations under Rule 16 and in particular *Brady*. We believe the Department should carefully consider whether it must re-examine past cases to see whether potentially discoverable but undisclosed Rule 16 or *Brady* material was collected by the NSA, and take appropriate steps to ensure that it has complied with its discovery obligations in such cases. ~~(TS//SI//NF)~~

The Department took steps to respond [redacted] to discovery motions [redacted]

However, the Department's handling of these motions did not require the Department to identify the potentially discoverable information derived under the Stellar Wind program that may exist in other cases. We recommend that the Department, in coordination with the NSA, develop and implement a procedure for identifying Stellar Wind-derived information that may be associated with international terrorism cases, currently pending or likely to be brought in the future, and to evaluate such information in light of the government's discovery obligations under Rule 16 and Brady. ~~(TS//STLW//SI//OC/NF)~~

CHAPTER EIGHT
PUBLIC STATEMENTS ABOUT THE SURVEILLANCE PROGRAM (U)

This chapter examines Attorney General Alberto Gonzales's testimony and public statements related to the Stellar Wind program. Aspects of this program were first disclosed publicly in a series of articles in The New York Times in December 2005. In response, the President publicly confirmed a portion of the Stellar Wind program – the interception of the content of international communications of people reasonably believed to have links to al Qaeda and related organizations. Subsequently, Attorney General Gonzales was questioned about the program in two hearings before the Senate Judiciary Committee in February 2006 and July 2007. ~~(S//NF)~~

In between those two hearings, former Deputy Attorney General James Comey testified before the Senate Judiciary Committee about the dispute between the Department and the White House concerning the program. Gonzales's and Comey's differing congressional testimony led to allegations that Gonzales had made misleading statements to Congress about the dispute and the program itself.[434] (U)

In this chapter, we examine whether Attorney General Gonzales made false, inaccurate, or misleading statements related to the Stellar Wind program. (U//~~FOUO~~)

I. Summary of the Dispute about the Program (U)

As described in detail in Chapters Three and Four, the Stellar Wind program is best understood as consisting of three types of collections, informally referred to as "baskets." Basket 1 related to the collection of e-mail and telephone content. Initially, the Stellar Wind program collected e-mail and telephone content when probable cause existed to believe one of the parties to the call or e-mail was outside the United States and at least one of the communicants was a member of an international terrorist group.

---

[434] For example, Senator Arlen Specter stated at a Senate hearing on July 24, 2007, that he did not find Attorney General Gonzales's testimony to be credible and suggested to the Attorney General that he "review this transcript very, very carefully." After this hearing Senate Judiciary Committee Chairman Patrick Leahy sent a letter to the OIG, dated August 16, 2007, asking the OIG to review Gonzales's statements to determine whether they were intentionally false, misleading, or inappropriate. Gonzales testified several times before the Senate and House Judiciary and Intelligence Committees about the program. In this chapter, we focus on his February 2006 and July 2007 testimony in which he discussed the events of March 2004. (U)

Basket 2 involved bulk collection of telephony meta data, and basket 3 involved bulk collection of e-mail meta data. (~~TS//STLW//SI//OC/NF~~)

These collections were authorized by a Presidential Authorization that was re-issued at approximately 30 to 45-day intervals. Each Authorization was certified as to form and legality by the Attorney General. The Attorney General's certifications were initially supported by legal opinions from OLC attorney John Yoo affirming the legality of the program. (~~TS//STLW//SI//OC/NF~~)

As discussed in Chapter Four, after Jack Goldsmith was confirmed as Assistant Attorney General for OLC in October 2003, he, along with Associate Deputy Attorney General Patrick Philbin, conducted an analysis of the legal basis underlying each basket in the Stellar Wind program. As a result of this review, he, Philbin, and recently confirmed Deputy Attorney General Comey concluded that they could find no legal support for several aspects of the existing program. [redacted] (~~TS//STLW//SI//OC/NF~~) [redacted]

In early March 2004, the dispute between the Department and the White House over the Department's revised legal analysis of the Stellar Wind program came to a head. Deputy Attorney General Comey, who assumed the duties of the Attorney General when Attorney General Ashcroft was hospitalized, informed the White House that the Department could not recertify the program. This dispute culminated in the unsuccessful attempt by then-White House Counsel Gonzales and White House Chief of Staff Andrew Card to get Attorney General Ashcroft to overrule Comey and recertify the program while he was in the hospital. When Ashcroft refused to certify the program and said that Comey was acting as the Attorney General, not him, the President reauthorized the program without the

Attorney General's certification. Instead Gonzales, as White House Counsel, recertified the program. ~~(TS//SI//NF)~~

After the White House's actions to continue the program without Justice Department certification, Deputy Attorney General Comey, FBI Director Mueller, and many other senior Department officials considered resigning. When the President learned of this, he directed that the Department work with other involved agencies and the White House to place the program on a firmer legal foundation. [redacted]

~~(TS//STLW//SI//OC/NF)~~

II. The New York Times Articles and President Bush's Confirmation Regarding NSA Activities (U)

In 2004, aspects of the Stellar Wind program were disclosed to two reporters for The New York Times. The reporters, James Risen and Eric Lichtblau, sought to publish an article about the program in late 2004. However, after a series of meetings with Administration officials who argued that publication of the story would harm the national security, The New York Times agreed to delay publishing the story. ~~(S//NF)~~

The New York Times eventually published a series of articles about the program on December 16 through 19, 2005. According to one of the reporters, the Times decided to publish the articles at least in part because the newspaper learned of serious concerns about the legality of the program that had "reached the highest levels of the Bush Administration."[435] (U)

The first article, on December 16, 2005, was entitled, "Bush Lets U.S. Spy on Callers Without Courts." This article stated that "Months after the Sept. 11 attacks, President Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying, according to government officials." The article described in broad terms the content collection aspect of the NSA program (basket 1), stating that according to officials the NSA has "monitored the international telephone calls of hundreds, perhaps

[435] See Eric Lichtblau, *Bush's Law* (2008), p. 203. (U)

thousands, of people inside the United States without warrants over the past three years in an effort to track possible 'dirty numbers' linked to al Qaeda." The article stated that the NSA continued to seek warrants to monitor purely domestic communications. ~~(TS//STLW//SI//OC/NF)~~

The article asserted that "reservations about aspects of the program" had also been expressed by Senator Jay Rockefeller (the Vice Chair of the Senate Select Committee on Intelligence) and a judge who presided over the FISA Court. The article added, "Some of the questions about the [NSA's] new powers led the administration to temporarily suspend the operation last year and impose more restrictions, officials said." The article also stated that "In mid-2004, concerns about the program expressed by national security officials, government lawyers and a judge prompted the Bush administration to suspend elements of the program and revamp it." However, the article incorrectly tied this suspension of the program to Judge Colleen Kollar-Kotelly's concerns that information gained from the program was also being used to seek FISA orders, rather than to the March 2004 dispute between Department officials and the White House about the legality of aspects of the program. ~~(TS//SI//NF)~~

On December 17, 2005, the day after The New York Times published the first article, President Bush publicly acknowledged the portion of the NSA program that was described in the article. President Bush described in broad terms these NSA electronic surveillance activities, stating:

> In the weeks following the terrorist attacks on our nation, I authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations. Before we intercept these communications, the government must have information that establishes a clear link to these terrorist networks.
>
> This is a highly classified program that is crucial to our national security. Its purpose is to detect and prevent terrorist attacks against the United States, our friends and allies. Yesterday the existence of this secret program was revealed in media reports, after being improperly provided to news organizations. As a result, our enemies have learned information they should not have, and the unauthorized disclosure of this effort damages our national security and puts our citizens at risk. Revealing classified information is illegal, alerts our enemies, and endangers our country . . . .
>
> The activities I authorized are reviewed approximately every 45 days. Each review is based on a fresh intelligence assessment of terrorist threats to the continuity of our government and the

threat of catastrophic damage to our homeland. During each assessment, previous activities under the authorization are reviewed. The review includes approval by our nation's top legal officials, including the Attorney General and the Counsel to the President. I have reauthorized the program more than 30 times since the September 11th attacks, and I intend to do so for as long as our nation faces a continuing threat from al Qaeda and related groups.[436] (U)

III. Other Administration Statements (U)

On January 19, 2006, the Justice Department issued a document, informally referred to as a "White Paper," entitled "Legal Authorities Supporting the Activities of the National Security Agency Described by the President." The 42-page document addressed in an unclassified form the legal basis for the collection activities that were described in the December 16, 2005, New York Times article and other media reports and confirmed by President Bush. The White Paper stated that the President acknowledged that "he has authorized the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or other related terrorist organizations." (U)

The White Paper reiterated the legal theory advanced by the Department in Goldsmith's May 2004 memorandum about the revised NSA program, which concluded that the September 18, 2001, Congressional Authorization for the Use of Military Force authorized the President to employ "warrantless communications intelligence targeted at the enemy," a fundamental incident of the use of military force, pursuant to the President's Article II Commander-in-Chief powers. The White Paper also argued that the NSA's activities were consistent with FISA, as confirmed and supplemented by the AUMF. ~~(TS//SI//NF)~~

On January 22, 2006, the White House also issued a press release and memorandum to counter criticism of the NSA program by members of Congress. The press release was entitled "Setting the Record Straight: Democrats Continue to Attack the Terrorist Surveillance Program." This document was the first time we found any official use of the term "Terrorist Surveillance Program" to apply to the NSA program or aspects of the program.[437] ~~(S//NF)~~

---

[436] The full text of President Bush's December 17, 2005, radio address can be found at http://www.whitehouse.gov/news/releases/2005/12/print/20051217.html. (U)

[437] See http://www.whitehouse.gov/news/releases/2006/01/200060122.html. We found that the term was used in the media prior to this time. The first published reference (Cont'd.)

The following day, on January 23, 2006, President Bush referred to the "terrorist surveillance program" during a speech at Kansas State University:

> Let me talk about one other program . . . something that you've been reading about in the news lately. It's what I would call a terrorist surveillance program. (U)

In the speech, President Bush described the program as the interception "of certain communications emanating between somebody inside the United States and outside the United States; and one of the numbers would be reasonably suspected to be an al Qaeda link or affiliate." (U)

On January 24, 2006, Attorney General Gonzales delivered a speech at the Georgetown University Law Center which, according to his prepared remarks, began by stating that his remarks "speak only to those activities confirmed publicly by the President, and not to purported activities described in press reports." Gonzales referred to the program throughout his speech as either the "terrorist surveillance program" or "the NSA's terrorist surveillance program." (U)

IV. Testimony and Other Statements (U)

After the New York Times articles disclosed aspects of the NSA program, members of Congress expressed concern that the President had exceeded his authority by authorizing electronic surveillance activity without FISA orders, and congressional hearings were held on the issue. Gonzales testified before the Senate Judiciary Committee on February 6, 2006, and July 24, 2007, about the NSA's surveillance activities. We describe in the next sections his testimony and other statements he made about the NSA's activities, as well as testimony by former Deputy Attorney General Comey before the Senate Judiciary Committee on May 15, 2007. ~~(TS//SI//NF)~~

---

we found to the "terrorist surveillance program" in connection with the NSA electronic surveillance activities was in NewsMax, an online news website, on December 22, 2005. (U) See "Barbara Boxer: Bush Spy Hearings Before Alito," NewsMax.com, December 22, 2005, http://archive.newsmax.com/archives/ic/2005/12/22/173255.shtml. On January 20, 2006, the term appeared again on another Internet blog called "RedState." See "Making the case for the NSA terrorist surveillance program," at http://www.redstate.com/story/2006/1/20/92730 /0977. (U)

A. Gonzales's February 6, 2006, Senate Judiciary Committee Testimony (U)

In his opening statement before the Senate Judiciary Committee on February 6, 2006, Gonzales began by saying that his testimony would necessarily be limited:

> Before going any further, I should make clear what I can discuss today. I am here to explain the Department's assessment that the President's terrorist surveillance program is consistent with our laws and Constitution. I am not here to discuss the operational details of that program, or any other classified activity. The President has described the terrorist surveillance program in response to certain leaks, and my discussion in this open forum must be limited to those facts the President has publicly confirmed – nothing more. Many operational details of our intelligence activities remain classified and unknown to our enemy – and it is vital that they remain so. (U)

The questioning of Gonzales at this hearing focused primarily on the nature of the NSA surveillance activity and the legal basis for it.[438] Senator Charles Schumer asked Gonzales specifically about accounts of a disagreement within the Justice Department over the NSA program:

> SEN. SCHUMER: But it's not just Republican senators who seriously question the NSA program, but very high-ranking officials within the administration itself. Now, you've already acknowledged that there were lawyers in the administration who expressed reservations about the NSA program. There was dissent. Is that right?
>
> ATTY GEN. GONZALES: Of course, Senator. As I indicated, this program implicates very difficult issues. The war on terror has generated several issues that are very, very complicated.
>
> SEN. SCHUMER: Understood.
>
> ATTY GEN. GONZALES: Lawyers disagree.

---

[438] Neither the Chairman of the Senate Judiciary Committee at the time (Senator Specter), nor the Ranking Member (Senator Leahy), were read into the program or provided the underlying documents authorizing the program. Senator Leahy stated at the outset of the hearing that he and others had made a request to review the Presidential Authorizations and OLC memoranda about the program, but that these materials had not been provided to the Committee. (U)

APPROVED FOR PUBLIC RELEASE

SEN. SCHUMER: I concede all those points. Let me ask you about some specific reports. It's been reported by multiple news outlets that the former number two man in the Justice Department, the premier terrorism prosecutor, Jim Comey, expressed grave reservations about the NSA program, and at least once refused to give it his blessing. Is that true?

ATTY GEN. GONZALES: Senator, here's a response that I feel that I can give with respect to recent speculation or stories about disagreements. There has not been any serious disagreement, including – and I think this is accurate – there's not been any serious disagreement about the program that the President has confirmed.

There have been disagreements about other matters regarding operations, which I cannot get into. I will also say –

SEN. SCHUMER: But there was some – I'm sorry to cut you off. But there was some dissent within the administration, and Jim Comey did express at some point – that's all I asked you – some reservation.

ATTY GEN. GONZALES: The point I want to make is that, to my knowledge, none of the reservations dealt with the program that we're talking about today. They dealt with operational capabilities that we're not talking about today.

SEN. SCHUMER: I want to ask you again about – I'm just – we have limited time.

ATTY GEN. GONZALES: Yes, sir.

SEN. SCHUMER: It's also been reported that the head of the Office of Legal Counsel, Jack Goldsmith, a respected lawyer and professor at Harvard Law School, expressed reservations about the program. Is that true?

ATTY GEN. GONZALES: Senator, rather than going individual by individual –

SEN. SCHUMER: No, I think we're – this is –

ATTY GEN. GONZALES: – let me just say that I think differing views that have been the subject of some of these stories does not – did not deal with the program that I'm here testifying about today.

SEN. SCHUMER: But you are telling us that none of these people expressed any reservations about the ultimate program. Is that right?

> ATTY GEN. GONZALES: Senator, I want to be very careful here, because, of course, I'm here only testifying about what the President has confirmed. And with respect to what the President has confirmed, I believe – I do not believe that these DOJ officials that you're identifying had concerns about this program. (U)

Throughout the hearing, other Senators asked Gonzales questions relating to various aspects of the NSA program, and Gonzales would often qualify his answers by stating that he was not discussing activities beyond what the President had confirmed. However, in doing so Gonzales sometimes suggested that the NSA's activities under the program were limited to what the President had confirmed. In one exchange with Senator Leahy, for example, Gonzales suggested that the electronic surveillance activities the President had publicly confirmed were the only activities the President had authorized to be conducted. Specifically, in response to a series of questions from Senator Leahy regarding what activities beyond warrantless electronic surveillance Gonzales would deem legal under the Authorization for the Use of Military Force, Gonzales stated,

> Sir, I have tried to outline for you and the committee what the President has authorized, and that is all that he has authorized. . . . There is all kinds of wild speculation out there about what the President has authorized and what we're actually doing. And I'm not going to get into a discussion, Senator, about hypotheticals.[439] ~~(S//NF)~~

---

[439] On February 28, 2006, Gonzales wrote to Senator Specter to provide additional responses to questions that he had answered during his February 6 hearing and to clarify certain responses. Gonzales wrote that he confined his letter and testimony

> to the specific NSA activities that have been publicly confirmed by the President. Those activities involve the interception by the NSA of the contents of communications in which one party is outside the United States where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization (hereinafter, the "Terrorist Surveillance Program").

One response Gonzales sought to clarify was this response to Senator Leahy. Gonzales wrote:

> First, as I emphasized in my opening statement, in all of my testimony at the hearing I addressed – with limited exceptions – only the legal underpinnings of the Terrorist Surveillance Program, as defined above. I did not and could not address operational aspects of the Program or any other classified intelligence activities. So, for example, when I testified in response to questions from Senator Leahy, "Sir, I have tried to outline for you and the Committee what the President has authorized, and that is all that he has authorized," Tr. at 53, I was confining my remarks to the Terrorist

(Cont'd.)

In response to Senator Sam Brownback's question about whether the FISA application process would include "even these sort of operations we've read about data mining operations? Would that include those sorts of operations, or are those totally a separate type of field?" (U)

Gonzales responded:

> I'm not here to talk about that. Again, let me just caution everyone that you need to read these stories with caution. There is a lot of mumbling – I mean, mixing and mangling of activities that are totally unrelated to what the President has authorized under the terrorist surveillance program, and so I'm uncomfortable talking about other kinds of operations that might – that are unrelated to the terrorist surveillance program. (U)

B. Comey's May 15, 2007, Senate Judiciary Committee Testimony (U)

Former Deputy Attorney General Comey appeared before the Senate Judiciary Committee on May 15, 2007, in a hearing called to examine whether the Department had politicized the firing of U.S. Attorneys. Senator Schumer, who presided over the hearing, began the questioning by asking Comey about reports in the media that in March 2004 White House Counsel Gonzales and White House Chief of Staff Card had visited Attorney General Ashcroft in the hospital in an effort to override Comey's decision, made when he served as Acting Attorney General, not to certify a classified program. Comey was asked to recount the details of the incident. (U)

After prefacing his remarks by stating that he could not discuss classified information, Comey described the events of March 2004, including the confrontation between the Department and White House officials in Ashcroft's hospital room. In describing these events, Comey referred to a single classified program. For example, Comey testified that:

> In the early part of 2004, the Department of Justice was engaged – the Office of Legal Counsel, under my supervision, in a reevaluation both factually and legally of a particular classified program. And it was a program that was renewed on a regular basis and required signature by the Attorney General

---

Surveillance Program as described by the President, the legality of which was the subject of the February 6th hearing.

Gonzales also attempted to clarify a response he had given to Senator Leahy about when the first Presidential Authorization was signed. Gonzales wrote that "The President first authorized the [Terrorist Surveillance] Program in October 2001 . . . ." (U)

> certifying to its legality. And the – and I remember the precise date; the program had to be renewed by March the 11th, which was a Thursday, of 2004. And we were engaged in a very intensive reevaluation of the matter. (U)

Comey also testified that "as Acting Attorney General, I would not certify the program as to its legality, and explained our reasoning in detail, which I will not go into here, nor am I confirming it's any particular program." As detailed in Chapter Four, Comey then described from his perspective the incident in the hospital room and testified that after that incident "[t]he program was reauthorized without us, without a signature from the Department of Justice attesting as to its legality . . . ." (U)

C. Gonzales's June 5, 2007, Press Conference (U)

In light of Comey's statements, questions were raised about the accuracy of Gonzales's February 2006 testimony to the Senate Judiciary Committee. For example, in a press conference on June 5, 2007, called to announce the indictment of members of an international gang called MS-13, the first question a reporter asked Gonzales concerned Comey's testimony:

> REPORTER: Attorney General, last month Jim Comey testified about visits you and Andy Card made to John Ashcroft's hospital bed. Can you tell us your side of the story? Why were you there and did Mr. Comey testify truthfully about it? Did he remember it correctly?
>
> ATTY GEN. GONZALES: Mr. Comey's testimony related to a highly classified program which the President confirmed to the American people some time ago. Because it's on a classified program I'm not going to comment on his testimony. (U)

As discussed below, when later asked about this statement, Gonzales said that he had misspoke, and that he did not mean to say that Comey's testimony related to the program that the President confirmed. (U)

D. Gonzales's July 24, 2007, Senate Judiciary Committee Testimony (U)

Gonzales was again called to testify before the Senate Judiciary Committee on July 24, 2007. In advance of Gonzales's July 24 appearance, Senator Leahy sent Gonzales a letter advising him of the questions that would be asked at the hearing.[440] The letter referenced Gonzales's

---

[440] According to the letter, Senator Leahy took this step because in Gonzales's appearance before the Senate Judiciary Committee on April 19, 2007, to discuss the removal of nine U.S. Attorneys, Gonzales had responded to an estimated 100 questions that (Cont'd.)

February 6, 2006, testimony in which he stated that Department officials did not have "concerns about this program." The letter also referenced Comey's May 15 testimony concerning the incident in Ashcroft's hospital room in March 2004. The letter specifically advised Gonzales that he would be asked to "provide a full explanation for the legal authorization for the President's warrantless electronic surveillance program in March and April 2004." (U)

At the July 24 hearing, Gonzales was repeatedly questioned about alleged inconsistencies between his and Comey's accounts of the events of March 2004 and the NSA program. For example, Senator Specter asked:

> Let me move quickly through a series of questions – there's a lot to cover – starting with the issue that Mr. Comey raises. You said, quote, "There has not been any serious disagreement about the program." Mr. Comey's testimony was that Mr. Gonzales began to discuss why they were there to seek approval and he then says, quote, "I was very upset. I was angry. I thought I had just witnessed an effort to take advantage of a very sick man."
>
> First of all, Mr. Attorney General, what credibility is left for you when you say there's no disagreement and you're party to going to the hospital to see Attorney General Ashcroft under sedation to try to get him to approve the program?
>
> ATTY GEN. GONZALES: The disagreement that occurred and the reason for the visit to the hospital, Senator, was about other intelligence activities. It was not about the terrorist surveillance program that the President announced to the American people. (U)

At other points in the hearing, Gonzales stated that the dispute referred to "other intelligence activities," and not the "terrorist surveillance program." (U)

Senator Schumer also questioned Gonzales about his answer in the June 5 press conference in which he stated that Comey's testimony "related to a highly classified program which the President confirmed to the American people some time ago." Gonzales first responded that he would have to look at the question and his response from the press conference, and then he said "I'm told that what I'd in fact – here in the press

---

he could "not recall." Leahy wrote that he wanted to assist Gonzales with his preparation for the July 24 testimony to "avoid a repeat of that performance." (U)

conference – I did misspeak, but I also went back and clarified it with the reporter."[441] (U)

Gonzales then responded to Senator Schumer that "The President confirmed the existence of one set of activities," and that "Mr. Comey was talking about a disagreement that existed with respect to other intelligence activities. . . . Mr. Comey's testimony about the hospital visit was about other intelligence activities, disagreements over other intelligence activities. That's how we'd clarify it." (U)

Other Senators questioned Gonzales's responses on this issue. For example, Senator Feingold stated:

> With respect to the NSA's illegal wiretapping program, last year in hearings before this committee and the House Judiciary Committee, you stated that, quote, "There has not been any serious disagreement about the program that the President has confirmed," unquote, that any disagreement that did occur, quote, "did not deal with the program that I am here testifying about today," unquote, and that, quote, "The disagreement that existed does not relate to the program the President confirmed in December to the American people," unquote. (U)
>
> Two months ago, you sent a letter to me and other members of this committee defending that testimony and asserting that it remains accurate. And I believe you said that again today. Now, as you probably know, I'm a member of the Intelligence Committee. And therefore I'm one of the members of this committee who has been briefed on the NSA wiretapping program and other sensitive intelligence programs. I've had the opportunity to review the classified matters at issue here. And I believe that your testimony was misleading, at best. I am prevented from elaborating in this setting, but I intend to send you a classified letter explaining why I have come to that conclusion. (U)

Senator Whitehouse, also a member of the Intelligence Committee, similarly stated:

> Mr. Gonzales, let me just follow up briefly on what Senator Feingold was saying, because I'm also a member of both committees. And I have to tell you, I have the exact same

---

[441] Gonzales also testified that he did not speak directly to the reporter (Dan Eggen, from the Washington Post) to clarify the comment. Rather, Gonzales said he told a Department spokesperson to go back and clarify the statement to Eggen. (U)

perception that he does, and that is that if there is a kernel of truth in what you've said about the program which we can't discuss but we know it to be the program at issue in your hospital visit to the Attorney General, the path to that kernel of truth is so convoluted and is so contrary to the plain import of what you said, that I, really, at this point have no choice but to believe that you intended to deceive us and to lead us or mislead us away from the dispute that the Deputy Attorney General subsequently brought to our attention. So you may act as if he's behaving, you know, in a crazy way to even think this, but at least count two of us and take it seriously.[442] (U)

Gonzales also offered to answer a question about the terrorist surveillance program in closed session during this exchange with Senator Specter:

SEN. SPECTER: Going back to the question about your credibility on whether there was dissent within the administration as to the terrorist surveillance program, was there any distinction between the terrorist surveillance program in existence on March 10th, when you and the Chief of Staff went to see Attorney General Ashcroft, contrasted with the terrorist surveillance program which President Bush made public in December of 2005?

ATTY GEN. GONZALES: Senator, this is a question that I should answer in a classified setting, quite frankly, because now you're asking me to hint or talk – to hint about our operational activities. And I'd be happy to answer that question, but in a classified setting.

SEN. SPECTER: Well, if you won't answer that question, my suggestion to you, Attorney General Gonzales, is that you review this transcript very, very carefully. I do not find your testimony credible, candidly. When I look at the issue of credibility, it is my judgment that when Mr. Comey was testifying he was talking about the terrorist surveillance program and that inference arises in a number of ways, principally because it was such an important matter that led you and the Chief of Staff to Ashcroft's hospital room. . . . So my suggestion to you is that you review your testimony very carefully. The chairman's already said that the committee's

[442] According to a May 17, 2006, letter from the Director of National Intelligence, two other members of the Judiciary Committee – Senators Dianne Feinstein and Orrin Hatch – also had been briefed on the NSA program. (U)

going to review your testimony very carefully to see if your credibility has been breached to the point of being actionable. (U)

Near the end of the hearing Senator Schumer questioned Gonzales regarding the meeting at the White House with the "Gang of Eight" congressional leaders, just before Gonzales and Card went to Ashcroft's hospital room on March 10, 2004:

> SEN. SCHUMER: OK. But you testified to us that you didn't believe there was serious dissent on the program that the President authorized. And now you're saying they knew of the dissent and you didn't?
>
> ATTY GEN. GONZALES: The dissent related to other intelligence activities. The dissent was not about the terrorist surveillance program the President confirmed and . . .
>
> . . .
>
> SEN. SCHUMER: You said, sir – sir, you said that they knew that there was dissent. But when you testified before us, you said there has not been any serious disagreement. And it's about the same program. It's about the same exact program. You said the President authorized only one before. And the discussion – you see, it defies credulity to believe that the discussion with Attorney General Ashcroft or with this group of eight, which we can check on – and I hope we will, Mr. Chairman: that will be yours and Senator Specter's prerogative -- was about nothing other than the TSP. And if it was about the TSP, you're dissembling to this committee. Now was it about the TSP or not, the discussion on the eighth?
>
> ATTY GEN. GONZALES: The disagreement on the 10th was about other intelligence activities.
>
> SEN. SCHUMER: Not about the TSP, yes or no?
>
> ATTY GEN. GONZALES: The disagreement and the reason we had to go to the hospital had to do with other intelligence activities.
>
> SEN. SCHUMER: Not the TSP? Come on. If you say it's about "other," that implies not. Now say it or not.
>
> ATTY GEN. GONZALES: It was not. It was about other intelligence activities.
>
> SEN. SCHUMER: Was it about the TSP? Yes or no, please? That's vital to whether you're telling the truth to this committee.

ATTY GEN. GONZALES: It was about other intelligence activities. (U)

When we interviewed Gonzales, he stated that there was never any intent to hide the NSA program from Congress, and he said that Congress was briefed on multiple occasions about the program.[443] Gonzales also stated that he could not explain to the Senate Judiciary Committee that the "serious" dispute concerned [redacted] Gonzales said that he could not recall where the term "terrorist surveillance program" originated, but that when he used the term it referred only to the content collection activities the President had confirmed publicly, and that the rest of the program remained classified. Gonzales also asserted that this distinction should have been clear to those on the committee who were read into the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

E. FBI Director Mueller's July 26, 2007, House Committee on the Judiciary Testimony (U)

Two days after Gonzales's July 24, 2007, Senate Judiciary Committee testimony, FBI Director Mueller testified before the House Judiciary Committee. At this hearing, Mueller was asked about his conversation with Attorney General Ashcroft at the hospital on the evening of March 10, 2004. As discussed in Chapter Four of this report, Mueller arrived at the hospital just after Gonzales and Card left. Mueller was asked to recount what he learned from Ashcroft concerning Ashcroft's exchange with Gonzales and Card earlier that evening:

REP. JACKSON LEE: Could I just say, did you have an understanding that the discussion was on TSP?

MR. MUELLER: I had an understanding the discussion was on a – a NSA program, yes.

REP JACKSON LEE: I guess we use "TSP," we use warrantless wiretapping, so would I be comfortable in saying that those were the items that were part of the discussion?

---

[443] Gonzales cited in particular the "Gang of Eight" briefing convened on March 10, 2004, to inform congressional leaders of the Department's legal concerns about aspects of the program and the need for a legislative fix. We also reviewed Gonzales's closed-session testimony before the House Permanent Select Committee on Intelligence (HPSCI), which he provided on July 19, 2007, just a few days before his July 24 Senate Judiciary Committee testimony. In his classified HPSCI testimony, Gonzales stated, "This disagreement [with Justice Department officials] primarily centered on [redacted] ~~(TS//STLW//SI//OC/NF)~~

MR. MUELLER: I – the discussion was on a national – an NSA program that has been much discussed, yes. (U)

We asked Mueller about his understanding of the term "terrorist surveillance program." Mueller said that the term "TSP" was not used by the FBI prior to The New York Times article and the President's confirmation of one aspect of the program. Mueller said he understood the term to refer to what the President publicly confirmed as to content intercepts. Mueller said he believed the term "TSP" was part of the "overarching" Stellar Wind program, but that "TSP" is not synonymous with Stellar Wind.[444] ~~(S//NF)~~

F. Gonzales's Follow-up Letter to the Senate Judiciary Committee (U)

In an effort to clarify his July 24, 2007, Senate testimony, on August 1, 2007, Gonzales sent unclassified letters to Judiciary Committee Chairman Leahy and Senator Specter. Gonzales's letter to Leahy stated that he was deeply concerned with suggestions that his testimony was misleading and he was determined to address any such impression. He explained that "shortly after 9/11, the President authorized the NSA to undertake a number of highly classified activities," and that, "although the legal bases for these activities varied, all of them were authorized in one presidential order, which was reauthorized approximately every 45 days." Gonzales wrote that before December 2005 "the term 'Terrorist Surveillance Program' was not used to refer to these activities, collectively or otherwise." Rather, Gonzales wrote that the term was first used in early 2006 "as part of the public debate that followed the unauthorized disclosure [by the New York Times] and the President's acknowledgement of one aspect of the NSA activities[.]" (U)

---

[444] We also interviewed an NSA official, who serves as an original classifying authority for the NSA, about the use of the term "terrorist surveillance program" or "TSP" at the NSA. [redacted]

~~(TS//STLW//SI//OC/NF)~~

Gonzales also wrote in this letter that in his July 24 testimony he was discussing "only that particular aspect of the NSA activities that the President has publicly acknowledged, and that we have called the Terrorist Surveillance Program[.]" He wrote that he recognized that his use of this term or his shorthand reference to the "'program' publicly 'described by the President'" may have "created confusion." Gonzales maintained that there was "not a serious disagreement between the Department and the White House in March 2004 about whether there was a legal basis for the particular activity later called the Terrorist Surveillance Program." (U)

Gonzales also wrote in his letter, "That is not to say that the legal issues raised by the Terrorist Surveillance Program were insubstantial; it was an extraordinary activity that presented novel and difficult issues and was, as I understand, the subject of intense deliberations within the Department. In the spring of 2004, after a thorough reexamination of all these activities, Mr. Comey and the Office of Legal Counsel ultimately agreed that the President could direct the NSA to intercept international communications without a court order where the interceptions were targeted at al Qaeda or its affiliates. Other aspects of the NSA's activities referenced in the DNI's letter [attached to Gonzales's letter] did precipitate very serious disagreement." (U)

V. OIG Analysis (U)

In this section, we assess whether Gonzales made false, inaccurate, or misleading statements during his testimony before the Senate Judiciary Committee. As discussed below, we concluded that Gonzales's testimony did not constitute a false statement under the criminal statutes. We also concluded that he did not intend his testimony to be inaccurate, false, or misleading. However, we found in at least two important respects his testimony was confusing, inaccurate, and had the effect of misleading those who were not read into the program. (U)

At the outset, we recognize that Gonzales was in a difficult position because he was testifying in an open, unclassified forum about a highly classified program. In this setting, it would be difficult for any witness to clearly explain the nature of the dispute between the White House and the Department while not disclosing additional details about classified activities, particularly because only certain NSA activities had been publicly confirmed by the President. (U)

However, some of this difficulty was attributable to the White House's decision not to brief the Judiciary Committee, which had oversight of the Department of Justice, about the program. As discussed in Chapter Four, the strict controls over the Department's access to the program hindered the

Department's ability to adequately fulfill its legal responsibilities concerning the program through March 2004. Similarly, the White House's decision not to allow at least the Chair and Ranking Members of the House and Senate Judiciary Committees to be briefed into the program created difficulties for Gonzales when he testified before Congress about the disputes regarding the program. This limitation also affected the Committee's ability to understand or adequately assess the program, especially in connection with the March 2004 dispute. We agree with Goldsmith's observation about the harm in the White House's "over-secrecy" for this program, as well as Director Mueller's suggestion, made in March 2004, that briefings on the program should have been given to the House and Senate Judiciary Committees. This did not occur, and it made Gonzales's testimony to the Senate Judiciary Committee unusually difficult. ~~(TS//SI//NF)~~

Yet, even given these difficulties, we believe that Gonzales's testimony was imprecise, confusing, and likely to lead those not read into the program to draw wrong conclusions about the nature of the dispute between White House and Department officials in March 2004. In addition, two Senators who had been read into the program stated that they were confused by Gonzales's testimony. Although we concluded that Gonzales did not intend to mislead Congress, his testimony nonetheless had the effect of creating confusion and inaccurate perceptions about certain issues covered during his hearings. (U)

Gonzales, as a participant in the March 2004 dispute between the White House and the Justice Department and, more importantly, as the nation's chief law enforcement officer, had a duty to balance his obligation not to disclose classified information with the need not to be misleading in his testimony about the events that nearly led to mass resignations of senior officials at the Justice Department and the FBI. Instead, Gonzales's testimony only deepened the confusion among members of Congress and the public about these matters. We were especially troubled by Gonzales's testimony at the July 2007 Senate hearing because it related to an important matter of significant public interest and because he had sufficient time to prepare for this hearing and the questions he knew he would be asked. (U)

At the outset of his testimony on February 6, 2006, Gonzales explained that he was confining his remarks to the program and the facts that the President publicly confirmed in his radio address on December 17, 2005. In those remarks, the President had, in essence, confirmed the

content collection part, or basket 1, of the NSA surveillance program.[445] The President, and Gonzales, used the term "terrorist surveillance program" in connection with the President's confirmation of these NSA activities. However, as discussed below, it was not clear – even to those read into the program – whether the term "terrorist surveillance program" referred only to content collection (basket 1) or the entire program.
~~(TS//STLW//SI//OC/NF)~~

Nevertheless, Gonzales suggested in his testimony that the dispute between the White House and the Department concerned other intelligence activities that were unrelated to the content collection portion of the program that the President had confirmed. This was not accurate. ~~(S//NF)~~

We recognize that the term "terrorist surveillance program" was intended by Gonzales and other Administration officials to describe a limited set of activities within the Stellar Wind program and that the term was created only in response to public disclosures about the program. However, by using phrases such as the "terrorist surveillance program" or "the program that the President has confirmed," and setting that program distinctly apart from "other intelligence activities," Gonzales's testimony created a perception that the two sets of activities were entirely unrelated, which was not accurate. Gonzales's testimony suggested that the dispute that Comey testified about was not related to the program that the President had confirmed, and instead that the dispute concerned unrelated "operations" or "intelligence activities." Thus, while Gonzales may have intended the term "terrorist surveillance program" to cover only content collection (basket 1), it led to confusion and misperceptions when he testified that the dispute [redacted] was unrelated to "the terrorist surveillance program."
~~(TS//STLW//SI//OC/NF)~~

Gonzales reinforced this misperception throughout his testimony. For example, when asked by Senator Leahy what activities Gonzales believed would be supported under the Authorization for Use of Military Force rationale, Gonzales stated, "I have tried to outline for you and the committee what the President has authorized, and that is all that he has authorized." In fact, the President had authorized two other types of collections in the same Authorization. Gonzales himself subsequently realized that his response to Senator Leahy was problematic. In a February 28, 2006, letter to Senators Specter and Leahy, Gonzales sought to clarify his response,

[445] [redacted]

stating, "I was confining my remarks to the Terrorist Surveillance Program as described by the President, the legality of which was the subject of the February 6th hearing." However, in our view this attempt to clarify his remarks did not go nearly far enough. As discussed below, it was not until after Gonzales's next appearance before the Senate Judiciary Committee in July 2007 that Gonzales acknowledged that the President had also authorized a range of intelligence-gathering activities, including those described under the terrorist surveillance program, in a single order. ~~(TS//STLW//SI//OC/NF)~~

We concluded that Gonzales created a misimpression for Congress and the public by suggesting that the March 2004 dispute between the Department and the White House concerned issues wholly unrelated to "the program the President confirmed," or the terrorist surveillance program. We believe a fairer and more accurate characterization would have been that the March 2004 dispute concerned aspects of a larger program of which the terrorist surveillance program was a part. As discussed earlier, the NSA viewed the three types of collections as a single program. The three types of collections were all authorized by the same Presidential order and administered by a single intelligence agency. Moreover, all three collections were known in the Intelligence Community by the same Top Secret/Sensitive Compartmented Information program cover term, Stellar Wind. ~~(TS//STLW//SI//OC/NF)~~

In addition, we believe that Gonzales's testimony regarding the dispute between the Department and the White House [redacted] was incomplete and not accurate. ~~(TS//SI//OC/NF)~~

When Senator Schumer asked Gonzales at the February 2006 Senate hearing whether media accounts that Comey "expressed grave reservations about the NSA program" were true, Gonzales responded that there was no "serious disagreement about the program that the President has confirmed." But there was a dispute about [redacted] As recounted in detail in Chapter Four of this report, [redacted] The dispute involving [redacted] was not resolved, and the March 11, 2004,

Presidential Authorization continued to permit the activity [redacted] ~~(TS//STLW//SI//OC/NF)~~

When we interviewed Gonzales, he told us that he was trying to be careful during his public testimony about discussing or characterizing a classified program with persons not read into the program, and that he used the term "serious disagreement" to distinguish the disagreement regarding [redacted] from other disagreements regarding the program. Gonzales told us that he believed his statement that there was "no serious disagreement" was accurate because he did not consider the Department's conclusion that [redacted] to be a point of "serious disagreement" between the Justice Department and the White House, particularly when compared to the more serious disagreement related to [redacted].[446] Gonzales also told the OIG that he would not have gone to Ashcroft's hospital room solely over [redacted] and other evidence discussed in Chapter Four tends to confirm that [redacted] was not the critical issue in the confrontation with Department officials at the hospital or that it precipitated the threat of mass resignations by senior Department and FBI officials. ~~(TS//STLW//SI//OC/NF)~~

Yet, even if one agrees that [redacted] was not a "serious disagreement" between the Department and the White House, Gonzales's testimony is still problematic. When Senator Schumer pressed Gonzales on whether Department officials "expressed any reservations about the ultimate program," Gonzales replied: "Senator, I want to be very careful here, because, of course, I'm here only testifying about what the President has confirmed. And with respect to what the President has confirmed, I believe – I do not believe that these DOJ officials that you're identifying had concerns about this program." ~~(TS//STLW//SI//OC/NF)~~

We understand that it is possible to construct an argument that the Department officials did not have "reservations" or "concerns" about the [redacted] However, while such an argument at best might be considered technically accurate, it would still not account for key details that were omitted from

[446] While Gonzales may subjectively have believed the disagreement about this issue did not rise to the level of a serious dispute, he was aware that Goldsmith and Addington sharply disagreed about [redacted] ~~(TS//SI//NF)~~

Gonzales's testimony that would be necessary for an accurate understanding of the situation. The Department clearly had reservations and concerns about the [redacted] of the program, [redacted] Moreover, Gonzales himself contradicted this attempted construction by stating in a February 28, 2006, letter to Senator Specter that the terrorist surveillance program was first authorized by the President in October 2001, years before the [redacted] Gonzales knew that Comey, Goldsmith, and others at the Department had expressed "reservations" or "concerns" about [redacted] prior to the President's decision to [redacted] ~~(TS//STLW//SI//OC/NF)~~

While we believe the evidence does show that [redacted] was more significant than the dispute about [redacted] the evidence is clear that Comey and others had strong and clearly identified concerns regarding the extent of the President's authority to conduct [redacted] These concerns had been communicated to the White House in several meetings over a period of months prior to and including March 2004, and the White House did not [redacted] part of the program in response to these concerns. However, Gonzales's testimony suggested that such concerns and reservations on the part of Justice Department officials never existed. To the contrary, the Department's firm objections to this aspect of the program were instrumental in bringing about [redacted] collection in "the program the President has confirmed." ~~(TS//STLW//SI//OC/NF)~~

Following his July 24, 2007, testimony, Gonzales acknowledged in an unclassified August 1, 2007, letter to Senator Leahy that his use of the term "terrorist surveillance program" and his "shorthand reference to the 'program' publicly 'described by the President' may have created confusion," particularly for those familiar with the full range of NSA activities authorized by the President. Gonzales wrote that he was determined to address any impression that his testimony was misleading. In this letter, Gonzales attempted to describe what he had meant by the term "terrorist surveillance program," stating that it covered one aspect of the NSA activities that the President had authorized. His letter also acknowledged the dispute concerned the legal basis for certain NSA activities that were regularly authorized in the same Presidential Authorization as the terrorist surveillance program. Gonzales also acknowledged that Comey had refused to certify a Presidential Authorization "because of concerns about the legal basis of certain of these NSA activities." Yet, this follow-up letter, while providing more context about the issues than his July 2007 statements, did not completely address the misimpressions created by his testimony.

Gonzales still suggested in his August 1 letter that the only dispute between the Department and the White House concerned aspects of the program [redacted] ~~(TS//STLW//SI//OC/NF)~~

While we again acknowledge the difficulty of the situation Gonzales faced in testifying publicly about a highly classified and controversial program, we believe Gonzales could have done other things to provide clearer and more accurate testimony without divulging classified information. Similar to the import of his August 1 letter, and without providing operational details about these other activities, he could have clarified that part of the dispute with the Department concerned the scope of what he called "the terrorist surveillance program," while another part of the dispute concerned other "intelligence activities" that were either related to the terrorist surveillance program or, more accurately, a different aspect of the same NSA program. Gonzales also could have explained that different activities under the program raised different concerns within the Department because each set of activities rested upon different legal theories.[447] ~~(S//NF)~~

Alternatively, Gonzales could have declined to discuss any aspect of the dispute at an open hearing.[448] Or, short of seeking a closed session, Gonzales could have sought White House approval to brief the Chairs and Ranking Members of the Senate and House Judiciary Committees about the program so that they would fully understand the nature of the NSA program and the classified issues surrounding the dispute. Instead, Gonzales gave public testimony that was confusing and inaccurate, and had the effect of misleading those who were not read into the program, as well as some who were. (U)

Concerning Gonzales's July 2007 testimony in particular, the questions Gonzales would be expected to answer were clearly foreseeable, especially in light of the disparities between his February 6, 2006, testimony and Comey's May 15, 2007, testimony. In addition, Gonzales had been provided a letter by Senator Leahy referencing Comey's testimony and advising Gonzales to be prepared to discuss the legal authorization for the "President's warrantless electronic surveillance program in March and April

[447] [redacted]

[448] As noted, Gonzales provided closed-session testimony before HPSCI on July 19, 2007, in which he described the March 2004 dispute between White House and Justice Department officials as [redacted] ~~(TS//STLW//SI//OC/NF)~~

2004." Gonzales was therefore on notice that he would be expected to bring clarity to the confusion that existed following Comey's testimony. Rather than clarify these matters, we believe Gonzales further confused the issues through his testimony. (U)

Finally, we considered whether Gonzales's testimony constituted criminal false statements and concluded that his statements did not constitute a criminal violation of 18 U.S.C. § 1001. A person violates that statute by "knowingly and willfully" making a "materially false, fictitious, or fraudulent statement or representation[.]" 18 U.S.C. § 1001(a)(2). We do not believe the evidence showed that Gonzales intended to mislead Congress or willfully make a false statement. Moreover, we do not believe a prosecutor could prove beyond a reasonable doubt that there was no interpretation of his words that could be viewed as literally true, even if his testimony was confusing and created misperceptions.[449] (U)

In sum, we believe that while the evidence did not show that Gonzales's statements constitute a criminal violation, or that he intended to mislead Congress, his testimony was confusing, not accurate, and had the effect of misleading those who were not knowledgeable about the program. His testimony also undermined his credibility on this important issue. As the Attorney General, we believe Gonzales should have taken more care to ensure that his testimony was as accurate as possible without revealing classified information, particularly given the significance of this matter and the fact that aspects of the dispute had been made public previously. (U)

---

[449] See *United States v. Milton*, 8 F.3d 39, 45 (D.C. Cir. 1993)("defense of literal truth" applies to false statement prosecutions under 18 U.S.C. § 1001), *cert. denied*, 513 U.S. 919 (1994). See also *United States v. Hsia*, 24 F. Supp. 2d 33 (D.D.C. 1998), in which the court stated, "A false statement is an essential element of a prosecution under 18 U.S.C. § 1001, and if the statement at issue is literally true a defendant cannot be convicted of violating Section 1001." Id. at 58; *United States v. Hsia*, 176 F.3d 517, 525 (D.C. Cir. 1999)(reversing on other grounds). (U)

CHAPTER NINE
CONCLUSIONS (U)

Within weeks of the terrorist attacks of September 11, 2001, the National Security Agency (NSA) initiated a Top Secret, compartmented program to collect and analyze international and domestic telephone and e-mail communications and related data. The intent of the NSA program, which used the cover term Stellar Wind, was to function as an "early warning system" to detect and prevent future terrorist attacks within the United States. ~~(TS//STLW//SI//OC/NF)~~

The program was authorized by the President in a series of Presidential Authorizations that were issued at approximately 30 to 45 day intervals and certified as to form and legality by the Attorney General. The Presidential Authorizations stated that an extraordinary emergency existed permitting the use of electronic surveillance within the United States for counterterrorism purposes, without a court order, under specified circumstances. Under the program the NSA collected vast amounts of information through electronic surveillance and other intelligence-gathering techniques, including information concerning the telephone and e-mail communications of American citizens and other U.S. persons. Top Secret compartmented information derived from this collection was provided to, among other agencies, the FBI, which sent Secret-level, non-compartmented versions of the information to FBI field offices as investigative leads. ~~(TS//STLW//SI//OC/NF)~~

The Stellar Wind program represented an extraordinary expansion of the NSA's signals intelligence activity and a departure from the traditional restrictions on electronic surveillance imposed under the Foreign Intelligence Surveillance Act (FISA), Executive Order 12333, and other laws. Yet, the program was conducted with limited notification to Congress and without judicial oversight, even as the program continued for years after the September 11 attacks. ~~(TS//STLW//SI//OC/NF)~~

The White House tightly controlled who within the Justice Department could be read into the Stellar Wind program. In particular, we found that only three Department attorneys, including the Attorney General, were read into the program and only one attorney was assigned to assess the program's legality in its first year and a half of operation. The limited number of Justice Department read-ins contrasted sharply with the hundreds of operational personnel who were read into the program at the FBI and other agencies involved with the program. ~~(TS//STLW//SI//OC/NF)~~

I. Operation of the Program (U//~~FOUO~~)

Under the program, the NSA initially intercepted the content of international telephone and e-mail communications in cases where at least one of the communicants was reasonably believed to be associated with any international terrorist group. These collections became known as basket 1 of the Stellar Wind program. [redacted] ~~(TS//STLW//SI//OC/NF)~~

The NSA also collected bulk telephony and e-mail meta data – communications signaling information showing contacts between and among telephone numbers and e-mail addresses, but not the contents of those communications. These collections became known as basket 2 (telephone meta data) and basket 3 (e-mail meta data) of the Stellar Wind program. ~~(TS//STLW//SI//OC/NF)~~

Under basket 2 collections, [redacted] These call detail records included the originating and terminating telephone number of each call, and the date, time, and duration of each call, but not the content of the call. The NSA collected [redacted] "pairs" of contacts per day, including all domestic and international telephone calls [redacted] ~~(TS//STLW//SI//OC/NF)~~

Regarding e-mail meta data (basket 3), the NSA collected and archived [redacted] Internet traffic [redacted][450] E-mail meta data included only the "to," "from," "cc," "bcc," and other addressing-type information, but similar to call detail records did not include the subject line or the message contents. ~~(TS//STLW//SI//OC/NF)~~

NSA analysts accessed baskets 2 and 3 for analytical purposes with specific telephone numbers or e-mail addresses that satisfied the standard

[450] [redacted]

for querying the data as described in the Presidential Authorizations. A small amount of the collected content and meta data was analyzed by the NSA, working with other members of the Intelligence Community, to generate intelligence reports about suspected terrorists and individuals possibly associated with them. Many of these reports were disseminated, or "tipped," to the FBI for further dissemination as leads to FBI field offices. As of March 2006, [redacted] individual U.S. telephone numbers [redacted] e-mail addresses had been tipped to the FBI, the vast majority of which were disseminated to FBI field offices for investigation or other action. The results of these investigations were uploaded into FBI databases. ~~(TS//STLW//SI//OC/NF)~~

The Justice Department had two primary roles in the Stellar Wind program. First, the Attorney General was required to certify each Presidential Authorization as to form and legality – in effect, to give the Department's assurance that the activities the President was authorizing the NSA to conduct were legal. In carrying out this responsibility, the Attorney General was advised by the Department's Office of Legal Counsel (OLC). As we described in this report and discuss in the next section, we found that during the early phase of the Stellar Wind program the Department lacked sufficient attorney resources to be applied to the legal review of the program and, due in significant part to the White House's extremely close hold over the program, was not able to coordinate its legal review of the program with the NSA. ~~(TS//STLW//SI//OC/NF)~~

The Department's other primary role in Stellar Wind was as a member of the Intelligence Community. The FBI was one of two main customers of the intelligence produced under the program (the other being the CIA). Working with the NSA, a small team of FBI personnel converted the NSA's Top Secret Stellar Wind intelligence reports into leads that were disseminated at the Secret level, under an FBI program called [redacted] to FBI field offices for appropriate action. As detailed in Chapter Six and discussed below, we concluded that although the information produced under the Stellar Wind program had value in some counterterrorism investigations, it played a limited role in the FBI's overall counterterrorism efforts. ~~(TS//STLW//SI//OC/NF)~~

II. Office of Legal Counsel's Analysis of the Stellar Wind Program ~~(TS//SI//NF)~~

As described in Chapters Three, Four, and Five of this report, the Justice Department advised the Executive Branch, and in particular the President, as to the legality of the Stellar Wind program. The Department's view of the legal support for the activities conducted under the program changed over time as more attorneys were read into the program. These

changes occurred in three phases. In the first phase of the program (September 2001 through May 2003), the legality of the program was founded on an analysis developed by John Yoo, a Deputy Assistant Attorney General in OLC. In the second phase (May 2003 through May 2004), the program's legal rationale underwent significant review and revision by OLC Assistant Attorney General Jack Goldsmith and Associate Deputy Attorney General Patrick Philbin. In the third and final phase (July 2004 through January 2007), based in part upon the legal concerns raised by the Department, the entire program was moved from presidential authority to statutory authority under FISA, with oversight by the FISA Court. ~~(TS//STLW//SI//OC/NF)~~

In Chapters Three and Four, we examined the Department's early role in assessing the legality of the Stellar Wind program. The Justice Department's access to the program was controlled by the White House, and former White House Counsel and Attorney General Alberto Gonzales told the OIG that the President decided whether non-operational personnel, including Department lawyers, could be read into the program. Department and FBI officials told us that obtaining approval to read in Department officials and FISA Court judges involved justifying the requests to Counsel to the Vice President David Addington and White House Counsel Gonzales, who effectively acted as gatekeepers to the read-in process for non-operational officials. In contrast, according to the NSA, operational personnel at the NSA, CIA, and the FBI were read into the program on the authority of the NSA Director, who at some point delegated this authority to the Stellar Wind Program Manager. ~~(TS//SI//NF)~~

We believe the White House's policy of limiting access to the program for non-operational personnel was applied at the Department of Justice in an unnecessarily restrictive manner prior to March 2004, and was detrimental to the Department's role in the operation of the program from its inception through that period. We also believe that Attorney General Ashcroft, as head of the Department during this time, was responsible for seeking to ensure that the Department had adequate attorney resources to conduct a thorough and accurate review of the legality of the program. We believe that the circumstances as they existed as early as 2001 and 2002 called for additional Department resources to be applied to the legal review of the program. As noted in Chapter Three, Ashcroft requested to have his Chief of Staff and Deputy Attorney General Larry Thompson read into the program, but the White House did not approve this request. However, because Ashcroft did not agree to be interviewed by the OIG for this investigation, we were unable to determine the full extent of his efforts to press the White House to read in additional Department officials between the program's inception in October 2001 and the critical events of March 2004. ~~(TS//SI//NF)~~

Although we could not determine exactly why Yoo remained the only Department attorney assigned to assess the program's legality from 2001 until his departure in May 2003, we believe that this practice represented an extraordinary and inappropriate departure from OLC's traditional review and oversight procedures and resulted in significant harm to the Department's role in the program. ~~(TS//SI//NF)~~

In the earliest phase of the program, Yoo advised Attorney General Ashcroft and the White House that the collection activities under Stellar Wind were a lawful exercise of the President's inherent authorities as Commander-in-Chief under Article II of the Constitution, subject only to the Fourth Amendment's reasonableness standard. In reaching this conclusion, Yoo dismissed as constitutionally incompatible with the President's Article II authority the FISA statute's provision that FISA was to be the "exclusive means" for conducting electronic surveillance in the United States for foreign intelligence purposes, and he concluded that these statutory provisions should be read to avoid conflicts with the President's constitutional Commander-in-Chief authority. (~~TS//STLW//SI//OC/NF~~)

As noted above, during the first year and a half of the Stellar Wind program only three Department attorneys were read into the program – Yoo, Attorney General Ashcroft, and James Baker, Counsel in the Office of Intelligence Policy and Review. Jay Bybee, the OLC Assistant Attorney General and Yoo's direct supervisor, was not read into the program and was unaware that Yoo was providing advice on the legal basis to support the program. Thus, Yoo was providing legal opinions on this unprecedented expansion of the NSA's surveillance authority without review by his OLC supervisor or any other Department attorney. Rather, Yoo worked alone on this project, and produced two major opinions supporting the legality of the program. ~~(TS//STLW//SI//OC/NF)~~

When additional attorneys were read into the program in 2003, they provided a fresh review of Yoo's legal memoranda. Patrick Philbin, an Associate Deputy Attorney General, and later Jack Goldsmith, Bybee's replacement as the Assistant Attorney General for OLC, concluded that Yoo's analysis was seriously flawed, both factually and legally. Goldsmith and Philbin concluded that Yoo's analysis fundamentally mischaracterized [redacted] by failing to address the fact that the NSA was collecting [redacted] and also failing to assess the legality of this activity as it was carried out by the NSA. Goldsmith and Philbin also pointed to Yoo's assertion that Congress had not sought to restrict presidential authority to conduct warrantless searches in the national security area, and criticized Yoo's omission from his analysis of a FISA provision (50 U.S.C. § 1811) that addressed the President's authority to conduct electronic surveillance during wartime. They further noted that Yoo based his assessment of the program's legality on an extremely

aggressive view of the law that revolved around the Constitutional primacy of the President's Article II Commander-in-Chief powers, and he may have done so based on a faulty understanding of key elements of the program. (~~TS//STLW//SI//OC/NF~~)

As described in Chapter Four, Goldsmith and Philbin's reassessment of the legality of Stellar Wind began after Yoo left the Department in May 2003, and culminated in a 108-page legal memorandum issued on May 6, 2004. That memorandum superseded Yoo's earlier Stellar Wind opinions and premised the legality of the program's electronic surveillance activities on statutory rather than Article II constitutional grounds.[451] As a consequence of this new legal rationale, Department officials concluded that the President's authority to conduct electronic surveillance of the enemy in wartime was [redacted] The Department's advice to the White House that the scope of collection under the program [redacted] was legally problematic led to a contentious dispute in March 2004 (discussed below in Section III). (~~TS//STLW//SI//OC/NF~~)

We agree with many of the criticisms offered by Department officials regarding the practice of allowing a single Department attorney to develop the legal justification for such a complex and contentious program without critical review both within the Department and by the NSA. These officials told us that errors in Yoo's legal memoranda may have been identified and corrected if the NSA had been allowed to review his work. They also stressed the importance of adhering to OLC's traditional practice of peer review of all OLC memoranda and the need for the OLC Assistant Attorney General, as a Senate-confirmed official, to review and approve all such opinions. (~~TS//SI//NF~~)

These officials also stated that such review and oversight measures are especially important with regard to legal opinions on classified matters that are not subjected to outside scrutiny. We agree with these officials' comments and note that because programs like Stellar Wind are not subject to the usual external checks and balances on Executive authority, OLC's advisory role is particularly critical to the Executive's understanding of potential statutory and Constitutional constraints on its actions. (~~TS//SI//NF~~)

[redacted]

(~~TS//STLW//SI//OC/NF~~)

We did not agree with Gonzales's view that it was necessary for national security reasons to limit the number of Department read-ins to those "who were absolutely essential," as distinguished from the numerous operational read-ins who were necessary to the technical implementation of the program. First, the program was as legally challenging as it was technically complex. Just as a sufficient number of operational personnel were read into the program to assure its proper technical implementation, we believe that as many attorneys as necessary should have been read in to assure the soundness of the program's legal foundation. This was not done during at least the first 20 months of the program. ~~(TS//SI//NF)~~

Second, we do not believe that reading in a few additional Department attorneys during the initial phase of the program would have jeopardized national security, especially given the [redacted] operational personnel who were cleared into the program during the same period.[452] In fact, the highly classified nature of the program, rather than constituting an argument for limiting the OLC read-ins to a single attorney, made the need for careful analysis and review within the Department and by the NSA more compelling. ~~(TS//SI//NF)~~

We also found that the expansion of legal thinking and breadth of expertise from reading in additional Department attorneys over time eventually produced more factually accurate and legally comprehensive analyses concerning the program. Increased attorney read-ins also was an important factor in grounding the program on firmer legal footing under FISA. The transition of the program from presidential authority to statutory authority under FISA with judicial oversight was made possible through the collective work of the attorneys who finally were read into the program beginning in 2004. The applications to the FISA Court to effectuate this transition were produced by Department attorneys, working with both legal and technical personnel at the NSA, further reinforcing our view that such coordinated efforts are more likely to produce well-considered legal strategies and analysis. ~~(TS//SI//NF)~~

In addition, as discussed in Chapters Six and Seven, the increase in the number of attorneys read into the program beginning in 2004 helped the Department to more efficiently "scrub" Stellar Wind-derived information in FISA applications and improve the handling of Stellar Wind-related discovery issues in international terrorism prosecutions. ~~(TS//STLW//SI//OC/NF)~~

---

[452] By the end of 2003, only Yoo, Ashcroft, Baker, Philbin, and Goldsmith had been read into Stellar Wind at the Department. [redacted] ~~(TS//SI//NF)~~

III. Hospital Visit and White House Recertification of the Program (U)

In Chapter Four, we describe how the Department's reassessment of Yoo's legal analysis led Deputy Attorney General James Comey, who was exercising the powers of the Attorney General while Ashcroft was hospitalized in March 2004, to conclude that he could not certify the legality of the Stellar Wind program. In response, the President sent Gonzales and Chief of Staff Andrew Card to visit Ashcroft in the hospital to seek his certification of the program, an action Ashcroft refused to take. We believe that the way the White House handled its dispute with the Department about the program – particularly in dispatching Gonzales and Card to Ashcroft's hospital room in an attempt to override Comey's decision – was troubling. ~~(TS//SI//NF)~~

As detailed in Chapter Four, by March 2004 when the Presidential Authorization in effect at that time was set to expire, Goldsmith had already notified the White House several months earlier about the Department's doubts concerning the legality of aspects of the Stellar Wind program. He had made clear that the Department questioned the legality of [redacted] ~~(TS//STLW//SI//OC/NF)~~

When Attorney General Ashcroft was hospitalized and unable to fulfill his duties, Deputy Attorney General Comey assumed the Attorney General's responsibilities. Before the Presidential Authorization was set to expire on March 11, 2004, Comey made clear to senior White House officials, including Vice President Cheney and White House Counsel Gonzales, that the Justice Department could not certify the program as legal. The White House disagreed with the Justice Department's position, and on March 10, 2004, convened a meeting of eight congressional leaders to brief them on the Justice Department's decision not to recertify the program and on the need to continue the program. The White House did not ask Comey or anyone from the Department to participate in this briefing, nor did it notify any Department officials that the briefing had been convened. ~~(TS//SI//NF)~~

Following this congressional briefing, at the direction of President Bush, Gonzales and White House Chief of Staff Andrew Card went to the hospital to seek Attorney General Ashcroft's certification of the Authorization. Again, the White House did not notify any Department officials, including Comey, the ranking Department official at the time, that it planned to take this action. Gonzales's and Card's attempt to persuade Attorney General Ashcroft, who was in the intensive care unit recovering from surgery and according to witnesses appeared heavily medicated, to certify the program over Comey's opposition was unsuccessful. Ashcroft

told Gonzales and Card from his hospital bed that he supported the Department's revised legal position, but that in any event he was not the Attorney General at the time – Comey was.[453] ~~(TS//SI//NF)~~

On March 11, the following day, Gonzales certified the Presidential Authorization as to form and legality. ~~(TS//SI//NF)~~

We agree with Director Mueller's observation that the White House's failure to have Justice Department representation at the congressional briefing and the attempt to persuade Ashcroft to recertify the Authorization without going through Comey "gave the strong perception that the [White House] was trying to do an end run around the Acting [Attorney General] whom they knew to have serious concerns as to the legality of portions of the program." ~~(TS//SI//NF)~~

After Mueller, Comey, and other senior Department and FBI officials made known their intent to resign, the President directed that the issue be resolved, and the program was modified to address the Department's legal concerns. Because we were unable to interview key White House officials, we could not determine for certain what caused the White House to change its position and modify the program, although we believe the prospect of mass resignations at the Department and the FBI was a significant factor in this decision. ~~(TS//SI//NF)~~

We reached several conclusions based on our review of the Department's role in the legal analysis of this program and the events surrounding the dispute between the Department and the White House. First, legal opinions supporting complex national security programs – especially classified programs that press the bounds of established law – should be collaborative products supported by sufficient legal and technical expertise and resources at the Department, working in concert with other participating agencies, with the goal of providing the Executive Branch the most informed and accurate legal advice. By limiting access to this program as it did, the White House undermined the Department's ability to perform its critical legal function. ~~(TS//SI//NF)~~

---

[453] Gonzales stated that even if he knew that Ashcroft was aware Comey opposed recertifying the program, Gonzales would still have wanted to speak with Ashcroft because he believed Ashcroft still retained the authority to certify the program. Gonzales testified before the Senate Judiciary Committee in July 2007 that although there was concern over Ashcroft's condition, "We would not have sought nor did we intend to get any approval from General Ashcroft if in fact he wasn't fully competent to make that decision." Gonzales also testified, "There's no governing legal principle that says that Mr. Ashcroft [. . .] If he decided he felt better, could decide, 'I'm feeling better and I can make this decision, and I'm going to make this decision.'" (U)

Second, we believe that if the OLC's traditional peer review and supervisory procedures had been adhered to at the outset, the prospect that aspects of the program would have rested on a questionable legal foundation for over 2 years would have been greatly mitigated. ~~(TS//SI//NF)~~

Third, we believe that the Department and FBI officials who resisted the pressure to recertify the Stellar Wind program because of their belief that aspects of the program were not legally supportable acted courageously and at significant professional risk. We believe that this action by Department and FBI officials – particularly Ashcroft, Comey, Mueller, Goldsmith, Philbin, and Counsel for Intelligence Policy James Baker – was in accord with the highest professional standards of the Justice Department. ~~(TS//SI//NF)~~

We recommend that when the Department of Justice is involved with such programs in the future, the Attorney General should carefully assess whether the Department has been given adequate resources to carry out its vital function as legal advisor to the President and should aggressively seek additional resources if they are found to be insufficient. We also believe that the White House should allow the Department a sufficient number of read-ins when requested, consistent with national security considerations, to ensure that such sensitive programs receive a full and careful legal review. (U)

IV. Transition of Program to FISA Authority ~~(TS//STLW//SI//OC/NF)~~

We also examined the transition of the Stellar Wind program's collection activities from presidential authority to FISA authority. We believe there were strong considerations that favored attempting to transition the program to FISA sooner than actually happened, especially as the program became less a temporary response to the September 11 attacks and more a permanent surveillance tool. ~~(TS//STLW//SI//OC/NF)~~

Chief among these considerations was the Stellar Wind program's substantial effect on privacy interests of U.S. persons. Under Stellar Wind, the government engaged in an unprecedented collection of information concerning U.S. persons. The President authorized the NSA to intercept, without judicial approval or oversight, the content of international communications involving many U.S. persons and the NSA collected massive amounts of non-content data about U.S. persons' domestic and international telephone calls and e-mail communications. We believe that such broad surveillance and collection activities, particularly for a significant period of time, should be conducted pursuant to statute and

judicial oversight. We also believe that placing these activities under Court supervision provides an important measure of accountability for the government's conduct that is less assured where the activities are both authorized and supervised by the Executive Branch alone.
~~(TS//STLW//SI//OC/NF)~~

The instability of the legal reasoning on which the program rested for several years and the substantial restrictions placed on FBI agents' access to and use of program-derived information due to Stellar Wind's highly classified status were additional reasons for transitioning Stellar Wind's collection activities to FISA authority. We acknowledge that the transition would always have been an enormously complex and time-consuming effort that rested upon novel interpretations and uses of FISA that not all FISA Court judges would authorize. Nevertheless, the events described in this report demonstrate that a full transition to FISA authority was achievable and, in our judgment, should have been pursued earlier.
~~(TS//STLW//SI//OC/NF)~~

V. Impact of Stellar Wind Information on FBI Counterterrorism Efforts (~~S//NF~~)

As a user of Stellar Wind program information, the FBI disseminated leads or "tippers" to FBI field offices. These tippers primarily consisted of specific domestic telephone numbers and e-mail addresses that NSA analysts had determined through meta data analysis were connected to individuals involved with al Qaeda or affiliated groups. The tippers also included content of communications intercepted by the NSA based upon its determination that there was probable cause to believe that a party to the communication was al Qaeda or an affiliated group. From October 2001 through February 2006, the NSA provided the FBI [redacted] Stellar Wind tippers, the vast majority of which were domestic telephone numbers.
~~(TS//STLW//SI//OC/NF)~~

The FBI's chief objective during the earliest months of Stellar Wind's operation was to expeditiously disseminate program information to FBI field offices for investigation, while protecting the NSA as the source of the information and the methods used to collect the information. The FBI assigned this task to a small group of personnel from the Telephone Analysis Unit (TAU) at FBI Headquarters. This group developed a straightforward process to receive the Top Secret, compartmented Stellar Wind reports from the NSA, reproduce the information in a non-compartmented, Secret-level format, and disseminate the information in Electronic Communications, or ECs, to the appropriate field offices for investigation. These [redacted] ECs placed restrictions on how the information could be used, instructing field offices that the information

was "for lead purposes only" and could not be used for any legal or judicial purpose. ~~(TS//STLW//SI//OC/NF)~~

The FBI's participation in Stellar Wind evolved over time as the program became less a temporary response to the September 11 attacks and more a permanent surveillance capability. As Stellar Wind continued to be reauthorized, the FBI tried to improve the effectiveness of its participation in the program. Most significantly, in February 2003 a team of FBI personnel (Team 10) was assigned to work full-time at the NSA to manage the FBI's participation in the program. ~~(TS//SI//NF)~~

Team 10's chief responsibility was to disseminate Stellar Wind information to FBI field offices. However, over time Team 10 began to participate in Stellar Wind in other ways. For example, Team 10 submitted telephone numbers and e-mail addresses to the NSA for possible querying against the bulk meta data collected under the program, and Team 10 regularly contributed to the NSA's drafting process for Stellar Wind reports. Overall, we found that the decision to assign Team 10 to the NSA improved the FBI's knowledge about Stellar Wind operations and gave the NSA better insight about how FBI field offices investigated Stellar Wind information. These benefits translated to improvements in the Stellar Wind report drafting process, and by extension, in [redacted] leads. ~~(TS//STLW//SI//OC/NF)~~

One of the other changes the FBI implemented to attempt to improve the process for handling Stellar Wind leads was to make the FBI's Headquarters-based Communications Analysis Unit (CAU), instead of the field offices, responsible for issuing National Security Letters (NSL) to obtain subscriber information on tipped telephone numbers and e-mail addresses. This measure, initiated in July 2003, was intended to address agent concerns that the leads, which reproduced the information in a non-compartmented, Secret-level format, did not provide sufficient information to initiate national security investigations, a prerequisite under Justice Department investigative guidelines to issuing NSLs. Agents complained that the ECs suffered from vagueness about the source of the information being provided and lacked factual details about the individuals allegedly involved with al Qaeda and with whom the domestic numbers being disseminated possibly were in contact. ~~(TS//STLW//SI//OC/NF)~~

We found that the CAU implemented this change by issuing NSLs from the [redacted] control file, the non-investigative file created in September 2002 as a repository for [redacted]-related communications between FBI Headquarters and field offices. Issuing NSLs from a control file instead of an investigative file was contrary to internal FBI policy. In November 2006, the FBI finally opened an investigative file for the [redacted] project. We believe the CAU and OGC officials involved in the decision

to issue NSLs from the [redacted] control file concluded in good faith that the FBI had sufficient predication either to connect the [redacted] NSLs with existing preliminary or full investigations of al Qaeda and affiliated groups or to open new preliminary or full investigations in compliance with Justice Department investigative guidelines. However, we concluded that the FBI could have, and should have, opened an investigative file for [redacted] when the decision was first made to have FBI Headquarters instead of field offices issue NSLs for [redacted] leads. ~~(TS//STLW//SI//OC/NF)~~

We also tried to assess the general role of Stellar Wind information in FBI investigations and its value to the FBI's overall counterterrorism efforts. Similar to the FBI, we had difficulty assessing the specific value of the program to the FBI's counterterrorism activities. ~~(S//NF)~~

The majority of Stellar Wind information the NSA provided the FBI related to domestic telephone numbers and e-mail addresses the NSA had identified through meta data analysis as having connections to al Qaeda or affiliated organizations. [redacted] Not surprisingly, FBI agents and analysts with experience investigating [redacted] leads told us that most leads were determined not to have any connection to terrorism. These agents and analysts did not identify for us any specific cases where [redacted] leads helped the FBI identify previously unknown subjects involved in terrorism, although we recognize that FBI officials and agents other than those we interviewed may have had different experiences with Stellar Wind information. ~~(TS//STLW//SI//OC/NF)~~

Two FBI statistical studies that attempted to assess the value of Stellar Wind meta data leads to FBI counterterrorism efforts did not reach explicit conclusions on the program's usefulness. The first study found that 1.2 percent of Stellar Wind leads made "significant" contributions.[454] The second study did not identify any examples of "significant" Stellar Wind contributions to FBI counterterrorism efforts.[455] The FBI OGC told us that

---

[454] As we described earlier in this chapter, the FBI considered a tipper "significant" if it led to any of three investigative results: the identification of a terrorist, the deportation from the United States of a suspected terrorist, or the development of an asset that can report about the activities of terrorists. ~~(S//NF)~~

[455] As described earlier in this chapter, the FBI considered a tipper "significant" if it led to any of three investigative results: the identification of a terrorist, the deportation from the United States of a suspected terrorist, or the development of an asset that can report about the activities of terrorists. ~~(TS//NF)~~

statements by senior FBI officials in congressional testimony that the Stellar Wind program had value were based in part on the results of the first study, which found that 1.2 percent of the Stellar Wind leads made significant contributions to FBI cases. ~~(TS//STLW//SI//OC/NF)~~

FBI agents we interviewed generally were supportive of Stellar Wind (or [redacted]), calling the information "one tool of many" in the FBI's anti-terrorism efforts that "could help move cases forward" by, for example, confirming a subject's contacts with individuals involved in terrorism or identifying additional terrorist contacts. However, FBI agents and analysts also told us that the Stellar Wind information disseminated to FBI field offices could also be frustrating because it often lacked details about the foreign individuals allegedly involved in terrorism with whom domestic telephone numbers and e-mail addresses were in contact. Some agents also believed that the [redacted] project failed to adequately prioritize leads sent to FBI field offices. ~~(TS//STLW//SI//OC/NF)~~

FBI Director Mueller told us that he believes the Stellar Wind program was useful and that the FBI must follow every lead it receives in order to prevent future terrorist attacks. He stated that to the extent such information can be gathered and used legally it must be exploited, and that he "would not dismiss the potency of a program based on the percentage of hits." Other witnesses shared this view that an intelligence program's value cannot be assessed by statistical measures alone. General Hayden said that the value of the program may lie in its ability to help the Intelligence Community determine that the terrorist threat embedded within the country is not as great as once feared. Some witnesses also believed that the value of the program should not depend on documented "success stories," but rather on maintaining an intelligence capability to detect potential terrorist activity in the future. Several witnesses suggested that the program provides an "early warning system" to allow the Intelligence Community to detect potential terrorist attacks, even if the system has not specifically uncovered evidence of preparations for such an attack.
~~(TS//STLW//SI//OC/NF)~~

As part of our analysis, we sought to look beyond these comments of general support for Stellar Wind to specific, concrete examples of the program's contributions that illustrated the role Stellar Wind information either has or could play in the FBI's counterterrorism efforts. We examined five cases frequently cited in documents we reviewed and during our interviews as examples of Stellar Wind's positive contributions to the FBI's counterterrorism efforts. The evidence indicated that Stellar Wind information had value in some of these investigations by causing the FBI to take action that led to useful investigative results. In other cases the connection between the Stellar Wind information and the FBI's investigative actions was more difficult to discern. ~~(TS//STLW//SI//OC/NF)~~

In the end, we found it difficult to assess or quantify the overall effectiveness of the Stellar Wind program to the FBI's counterterrorism activities. However, based on the interviews conducted and documents reviewed, we concluded that although Stellar Wind information had value in some counterterrorism investigations, it generally played a limited role in the FBI's overall counterterrorism efforts. ~~(S//NF)~~

It is also important to note that a significant consequence of the NSA program and the FBI's approach to assigning leads for program information was that FBI field offices conducted many threat assessments on individuals located in the United States, including U.S. persons, that typically were determined not to have any nexus to terrorism or represent a threat to national security. As a result, the FBI collected and retained a significant amount of personal information about the users of tipped telephone numbers and e-mail addresses, such as names and home addresses, places of employment, foreign travel, and the identity of family members. The results of these threat assessments and the information collected generally were reported in communications to FBI Headquarters and uploaded into FBI databases. ~~(TS//STLW//SI//OC/NF)~~

The FBI's collection of information in this manner is ongoing under [redacted] project, the successor FBI project to [redacted] which disseminates to FBI field offices lead information the NSA derives from bulk telephony and e-mail meta data now collected under FISA authority. Like [redacted] project requires FBI field offices to conduct threat assessments on telephone numbers and e-mail addresses identified through the NSA's analytical process that the FBI is not already aware of, including telephone numbers and e-mail addresses one or two steps removed from direct contacts with individuals involved in terrorism. To the extent the leads derived from the FISA-authorized activities generate results similar to those under Stellar Wind, the FBI threat assessments will continue to result in the collection and retention of a significant amount of personal information about individuals in the United States, including U.S. persons, who do not have a nexus to terrorism or represent a threat to national security. ~~(TS//STLW//SI//OC/NF)~~

We recommend that, as part of the [redacted] project, the Justice Department's National Security Division (NSD), working with the FBI, should collect information about the quantity of telephone numbers and e-mail addresses disseminated to FBI field offices that are assigned as Action leads and that require offices to conduct threat assessments. The information compiled by the Justice Department should include whether individuals identified in threat assessments are U.S. or non-U.S. persons and whether the threat assessments led to the opening of preliminary or full national security investigations. With respect to threat assessments that conclude that users of tipped telephone numbers or e-mail addresses are

not involved in terrorism and are not threats to national security, the Justice Department should take steps to track the quantity and nature of the U.S. person information collected and how the FBI retains and utilizes this information. This will enable the Justice Department and entities with oversight responsibilities, including the OIG and congressional committees, to assess the impact this intelligence program has on the privacy interests of U.S. persons and to consider whether, and for how long, such information should be retained. ~~(TS//SI//NF)~~

We also recommend that, consistent with NSD's current oversight activities and as part of its periodic reviews of national security investigations at FBI Headquarters and field offices, NSD should review a representative sampling [redacted] leads to those offices. For each lead examined, NSD should assess FBI compliance with applicable legal requirements in the use of the lead and in any ensuing investigations, particularly with the requirements governing the collection and use of U.S. person information. ~~(TS//SI//NF)~~

VI. Discovery and "Scrubbing" Issues ~~(TS//SI//NF)~~

Although Stellar Wind was conceived and implemented as an intelligence-gathering program, it was inevitable that the information from this program would intersect with the Department's prosecutorial functions, both in criminal cases brought in federal courts and in seeking FISA orders from the FISA Court. We found that the limited number of Department read-ins also had adverse consequences on issues related to these Department functions. ~~(TS//STLW//SI//OC/NF)~~

One such issue concerned the Department's compliance with discovery obligations in international terrorism prosecutions, which we discuss in Chapter Seven. We determined that the Department was aware as early as [redacted] that information collected under Stellar Wind could have implications for the Department's litigation responsibilities under Federal Rule of Criminal Procedure 16 and *Brady v. Maryland*, 373 U.S. 83 (1963). ~~(TS//STLW//SI//OC/NF)~~

Analysis of this discovery issue was first assigned to John Yoo in [redacted] Yoo, working alone, produced a legal analysis of the government's discovery obligations in the case of [redacted] and [redacted]

[redacted]

~~(TS//STLW//SI//OC/NF)~~

[redacted]

No Justice Department attorneys with terrorism prosecution responsibilities were read into the Stellar Wind program until mid-2004, and as a result the Department continued to lack the advice of attorneys who were best equipped to identify and examine the discovery issues in connection with the program. Since that time the Department has taken steps to respond [redacted] to [redacted] discovery motions [redacted] These responses involve the use of the Classified Information Procedures Act, 18 U.S.C. App. 3, to file *ex parte* in camera pleadings with federal courts to describe any potentially responsive Stellar Wind-derived information. [redacted]

[redacted] (~~TS//STLW//SI//OC/NF~~)

[redacted] we recommend that the Department assess its discovery obligations regarding Stellar Wind-derived information in international terrorism prosecutions. We also recommend that the Department carefully consider whether it must re-examine past cases to see whether potentially discoverable but undisclosed Rule 16 or *Brady* material was collected by the NSA under the program, and take appropriate steps to ensure that it has complied with its discovery obligations in such cases. We also recommend that the Department, in coordination with the NSA, implement a procedure to identify Stellar Wind-derived information that may be associated with international terrorism cases currently pending or likely to be brought in the future and evaluate whether such information should be disclosed in light of the

government's discovery obligations under Rule 16 and *Brady.* (~~TS//STLW//SI//OC/NF~~)

In addition, we examined the issue of the Department's use of Stellar Wind-derived information in FISA applications. We believe it was foreseeable that some Stellar Wind-derived information would be contained in the FISA applications filed by the Department's Office of Intelligence Policy and Review (OIPR). OIPR Counsel Baker believed, and we agree, that it would have been detrimental to this relationship if the Court learned that information from Stellar Wind was included in FISA applications without the Court being told so in advance. As discussed in Chapter Three, White House officials initially rejected the idea of reading in members of the FISA Court, but after Department officials continued to press the issue, ultimately in January 2003 agreed to read in a single judge in January 2002 (Presiding Judge Lamberth, followed by Presiding Judge Kollar-Kotelly in May 2002). ~~(TS//STLW//SI//OC/NF)~~

The "scrubbing" procedures imposed by the Court and implemented by Baker to account for Stellar Wind-derived information in international terrorism FISA applications created concerns among some OIPR attorneys about the unexplained changes being made to their FISA applications. These scrubbing procedures also substantially altered the assignment of cases to FISA Court judges for nearly 3 years. We concluded that once Stellar Wind began to affect the functioning of the FISA process shortly after the program's inception, the number of OIPR staff and FISA Court judges read into Stellar Wind should have increased. Instead, read-ins were limited to a single OIPR official for over two years and to the Presiding Judge of the FISA Court for a period of four years. (~~TS//STLW//SI//OC/NF~~)

The Justice Department, together with the FBI and the NSA, today continues to apply scrubbing procedures to international terrorism FISA applications. Since January 2006, all members of the Court have been briefed on the Stellar Wind program and all of the judges handle applications that involve Stellar Wind-derived information in FISA applications. While we found that the government has expended considerable resources to comply with the scrubbing procedures required by the FISA Court since February 2002, we did not find any instances of the government being unable to obtain FISA surveillance coverage on a target because of this requirement. (~~TS//STLW//SI//OC/NF~~)

VII. Gonzales's Statements (U)

As part of this review, the OIG examined whether Attorney General Gonzales made false or misleading statements to Congress related to the Stellar Wind program. We concluded that Gonzales's testimony did not

constitute a false statement and that he did not intend to mislead Congress. However, we concluded that his testimony in several respects was confusing, not accurate, and had the effect of misleading those who were not knowledgeable about the program. ~~(S//NF)~~

Aspects of the Stellar Wind program were first disclosed publicly in a series of articles in The New York Times in December 2005. In response, the President publicly confirmed a portion of the program – which he called the terrorist surveillance program – describing it as the interception of the content of international communications of people reasonably believed to have links to al Qaeda and related organizations (basket 1). Subsequently, Attorney General Gonzales was questioned about NSA surveillance activities in two hearings before the Senate Judiciary Committee in February 2006 and July 2007. ~~(TS//STLW//SI//OC/NF)~~

Through media accounts and former Deputy Attorney General Comey's Senate Judiciary Committee testimony in May 2007, it was publicly revealed that the Department and the White House had a major disagreement related to the program in March 2004. As discussed in Chapter Four, this dispute – which resulted in the visit to Attorney General Ashcroft's hospital room by Gonzales and Card and brought several senior Department and FBI officials to the brink of resignation after the White House continued the program [redacted] ~~(TS//STLW//SI//OC/NF)~~

In his testimony before the Senate Judiciary Committee, Gonzales stated that the dispute at issue between the Department and the White House did not relate to the "Terrorist Surveillance Program" that the President had confirmed, but rather pertained to other intelligence activities. We believe this testimony created the misimpression that the dispute concerned activities entirely unrelated to the terrorist surveillance program, which was not accurate. In addition, we believe Gonzales's testimony that Department attorneys did not have "reservations" or "concerns" about the program the "President has confirmed" was incomplete and confusing because Gonzales did not account for the fact that the Department's concerns were what led to [redacted] and that these concerns had been conveyed to the White House over a period of months prior to and including March 2004 when the issue was resolved. ~~(S//NF)~~

We recognize that Attorney General Gonzales was in the difficult position of testifying about a highly classified program in an open forum. However, we also believe that Gonzales, as a participant in the March 2004 dispute between the White House and the Justice Department and, more importantly, as the nation's chief law enforcement officer, had a duty to balance his obligation not to disclose classified information with the need

not to be misleading in his testimony about the events that nearly led to mass resignations of the most senior officials at the Justice Department and the FBI. Although we believe that Gonzales did not intend to mislead Congress, we believe his testimony was confusing, inaccurate, and had the effect of misleading those who were not knowledgeable about the program. ~~(TS//SI//NF)~~

VIII. Conclusion (U)

From the inception of the Stellar Wind program in October 2001, vast amounts of information about telephone and e-mail communications were collected and stored in databases at the NSA. The NSA used this information to conduct analysis and disseminate reports to support the government's counterterrorism efforts. We found that in the early years of the Stellar Wind program, the Department of Justice lacked the necessary legal resources to carry out an adequate review of the legality of the program. The White House strictly controlled the Department's access to the program. For the first year and a half of the program only 3 Department officials were read into Stellar Wind, and only 3 more officials had been read in by the end of 2003. Only a single Department attorney analyzed the legal basis for the program during its first year and a half of its operation. Beginning in mid-2003, after additional Department officials were read into the program, the Department determined that this attorney's initial legal analysis was legally and factually flawed. ~~(TS//STLW//SI//OC/NF)~~

We believe that the strict controls over the Department's access to the program undermined the role of the Justice Department in advising the President as to the legality of the program during its early phase of operation. The Department's comprehensive reassessment of the program's legality beginning in mid-2003 resulted in a contentious dispute with the White House that nearly led to the mass resignation of the Department's senior leadership. In March 2004 the White House continued the program despite the Department's conclusion that it found no legal support for aspects of the program. In the face of the potential resignations, however, the White House [redacted] in accord with the Department's legal concerns. Eventually, the entire program was transitioned, in stages, to the authority of the FISA statute. ~~(TS//STLW//SI//OC/NF)~~

Given the broad nature of the collection activities under the Stellar Wind program, the substantial amount of information the program collected related to U.S. persons, and the novel legal theories advanced to support the program, we believe that the Department should have more carefully and thoroughly reviewed the legality of the program, in accord with its normal

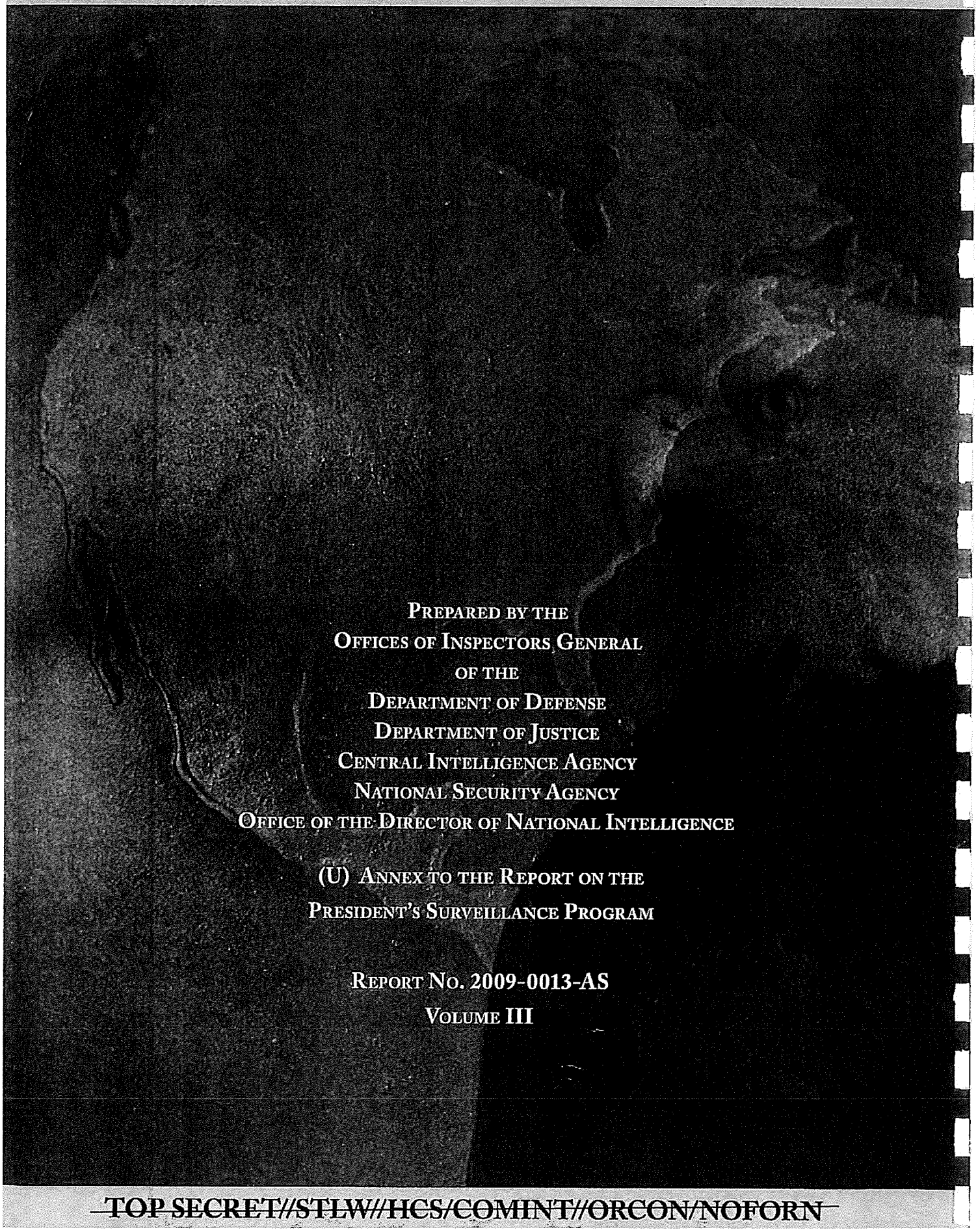
peer review and oversight practices, particularly during its first year and a half of operation. ~~(TS//STLW//SI//OC/NF)~~

We also concluded that the Department should have begun efforts to transition the Stellar Wind program to FISA authority earlier than March 2004, when that process began, especially as Stellar Wind became less a temporary response to the September 11 attacks and more a permanent surveillance tool. We believe that such broad surveillance and collection activities conducted in the United States that impact U.S. persons, particularly when they extend for such a significant period of time, should be conducted pursuant to statute and be subjected to judicial oversight. Placing such activities under Court supervision, as now occurs, also provides an important measure of accountability for the government's conduct that is less assured when the activities are authorized and supervised by the Executive Branch alone. ~~(TS//STLW//SI//OC/NF)~~

Finally, we believe that the Department should carefully monitor the collection, use, and retention of the information that is now collected under FISA authority, given the expansive scope of the collection activities. The Department and other agencies should also continue to examine the value of collecting such information to the government's ongoing counterterrorism efforts. ~~(TS//SI//NF)~~

APPROVED FOR PUBLIC RELEASE

APPROVED FOR PUBLIC RELEASE



PREPARED BY THE
OFFICES OF INSPECTORS GENERAL
OF THE
DEPARTMENT OF DEFENSE
DEPARTMENT OF JUSTICE
CENTRAL INTELLIGENCE AGENCY
NATIONAL SECURITY AGENCY
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

(U) ANNEX TO THE REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM

REPORT NO. 2009-0013-AS
VOLUME III

Approved for public release May 5, 2014

~~TOP SECRET//COMINT [redacted]//TSP//ORCON/NOFORN//MR~~

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION This Document Relates to: (1) All Actions Against the *MCI* and *Verizon* Defendants in the Master MCI and Verizon Consolidated Complaint, Dkt. 125; (2) *Bready*, et al. *v. Verizon Maryland* (06-06313); (3) *Chulsky* et al. *v. Cellco Partnership d/b/a Verizon Wireless* (06-06570); and (4) *Riordan*, et al. *v. Verizon Communications* (06-3574)	MDL Dkt. No. 06-1791-VRW **CLASSIFIED DECLARATION OF LT. GEN. KEITH B. ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY** **SUBMITTED *IN CAMERA*, *EX PARTE*** Hon. Vaughn R. Walker

(U) I, Lieutenant General Keith B. Alexander, do hereby state and declare as follows:

I. (U) Introduction

1. **(U)** I am the Director of the National Security Agency (NSA), an intelligence agency within the Department of Defense. I am responsible for directing the NSA, overseeing the operations undertaken to carry out its mission and, by specific charge of the President and the Director of National Intelligence, protecting NSA activities and intelligence sources and methods. I have been designated an original TOP SECRET classification authority under Executive Order No. 12958, 60 Fed. Reg. 19825 (1995), as amended on March 25, 2003, and Department of Defense Directive No. 5200.1-R, Information Security Program Regulation, 32 C.F.R. § 159a.12 (2000).

2. **(U)** The purpose of this declaration is to support an assertion of the military and state secrets privilege (hereafter "state secrets privilege") by the Director of National Intelligence (DNI) as the head of the intelligence community, as well as the DNI's assertion of a statutory privilege under the National Security Act. Specifically, in the course of my official duties, I

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: MR

Approved for public release May 5, 2014

have been advised of this litigation and the allegations in the various complaints in this action brought against the Verizon Defendants, including the MCI entities.[1] As described herein, various classified facts related to the Plaintiffs' claims are subject to the DNI's state secrets privilege assertion. The disclosure of this information, which relates to NSA intelligence information, activities, sources, and methods, reasonably could be expected to cause exceptionally grave damage to the national security of the United States. In addition, it is my judgment that sensitive state secrets are so central to the subject matter of the litigation that any attempt to proceed in the case risks the disclosure of the secrets described herein and exceptionally grave damage to the national security of the United States. Through this declaration, I also hereby invoke and assert the NSA's statutory privilege set forth in section 6 of the National Security Agency Act of 1959, Public Law No. 86-36 (codified as a note to 50 USC. § 402) ("NSA Act"), to protect the information related to NSA activities described below. The statements made herein are based on my personal knowledge of NSA activities and operations, and on information available to me as Director of the NSA.

II. (U) Summary

3. ~~(TS//SI[redacted]//TSP//OC/NF)~~ This lawsuit implicates several highly classified and critically important NSA intelligence activities and, in particular, [redacted] Although Plaintiffs wrongly claim that the NSA conducts a dragnet of surveillance of the content of millions of communications sent or received by people inside the United States, [redacted]

[redacted]

[1] (U) Any reference to "Verizon" in this declaration includes all Verizon Defendants in this matter. "Verizon" also specifically includes the MCI Defendants, which are now a part of Verizon, even though "MCI" may at times be referenced separately.

Approved for public release May 5, 2014

[redacted]

4. ~~(TS//SI~~ [redacted] ~~//TSP//OC/NF)~~ The protection of information about these activities, including the following, is vital to the national security of the United States: (1) [redacted] (2) any information concerning whether particular individuals such as the named Plaintiffs have been subject to any NSA intelligence activities; (3) program information about NSA intelligence activities, including facts demonstrating that the TSP was limited to al Qaeda-related international communications and was not a content surveillance dragnet; and (4) facts that would tend to confirm or deny the existence of the NSA's meta data activities. Any disclosure or official confirmation of this information would have exceptionally grave consequences for the national security. Critical foreign intelligence sources and methods would be compromised,

Approved for public release May 5, 2014

[redacted] and the ability of the United States to [redacted] would be severely damaged.

5. (U) For these reasons, as set forth further below, the state secrets and statutory privilege assertions that the DNI and I are making should be upheld and the information described in this declaration should be protected from disclosure. I also believe that any further litigation of this case poses exceptionally grave risks to the national security.

(U) Table of Contents

6. ~~(TS//SI [redacted]//TSP//OC/NF)~~ To facilitate the Court's review, this declaration is organized as follows:

I. Introduction

II. Summary

III. Classification of Declaration

IV. Background Information

A. The National Security Agency

B. September 11, 2001 and the Continuing al Qaeda Threat

V. Information Protected by Privilege

VI. Description of Information Subject to Privilege and the Harm of Disclosure

A. Information That May Tend to Confirm or Deny Whether Verizon/MCI Has Assisted the NSA with Any Alleged Intelligence Activities

[redacted]

Approved for public release May 5, 2014

[redacted]

B. Information That May Tend to Confirm or Deny Whether or Not the Plaintiffs Have Been Subject to Any Alleged NSA Activities That May Be at Issue in This Matter

1. [redacted]

2. [redacted]

3. Harm of Disclosure

C. Information Concerning NSA Activities, Sources, and Methods, and the Harm of Disclosure

1. Information Concerning Plaintiffs' Allegations of Content Surveillance

2. Information Concerning Meta Data Activities

3. Information Demonstrating the Success of TSP and Meta Data Activities

4. Information Concerning the FISC Orders

VII. Risks of Allowing Litigation to Proceed

VIII. Summary and Conclusion

III. (U) Classification of Declaration

7. ~~(S)~~ This declaration is classified TOP SECRET//COMINT [redacted]//TSP//ORCON/NOFORN//MR pursuant to the standards in Executive Order No. 12958, as amended by Executive Order No. 13292. Under Executive Order No. 12958, information is classified "TOP SECRET" if unauthorized disclosure of the information reasonably could be expected to cause exceptionally grave damage to the national security of the United States; "SECRET" if unauthorized disclosure of the information reasonably could be

Approved for public release May 5, 2014

expected to cause serious damage to national security; and "CONFIDENTIAL" if unauthorized disclosure of the information reasonably could be expected to cause identifiable damage to national security. At the beginning of each paragraph of this declaration, the letter or letters in parentheses designate(s) the degree of classification of the information the paragraph contains. When used for this purpose, the letters "U," "C," "S," and "TS" indicate respectively that the information is either UNCLASSIFIED, or is classified CONFIDENTIAL, SECRET, or TOP SECRET.[2]

8. ~~(S)~~ Additionally, this declaration also contains Sensitive Compartmented Information (SCI), which is "information that not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods." 28 C.F.R. § 17.18(a). Because of the exceptional sensitivity and vulnerability of such information, these safeguards and access requirements exceed the access standards that are normally required for information of the same classification level. Specifically, this declaration references communications intelligence (COMINT), also referred to as special intelligence (SI), which is a subcategory of SCI. COMINT or SI identifies SCI that was derived from exploiting cryptographic systems or other protected sources by applying methods or techniques, or from intercepted foreign communications.

[2] ~~(TS//SI//NF)~~ [redacted]

Approved for public release May 5, 2014

9. ~~(TS//SI-[redacted]//TSP//OC/NF)~~ This declaration also contains information related to or derived from the Terrorist Surveillance Program (TSP), a controlled access signals intelligence program authorized by the President in response to the attacks of September 11, 2001. Although the President publicly acknowledged the existence of the TSP in December 2005, details about the program remain highly classified and strictly compartmented. Information pertaining to this program is denoted with the special marking "TSP" and requires more restrictive handling. [redacted]

10. ~~(S)~~ In addition to the fact that classified information contained herein may not be revealed to any person without authorization pursuant to Executive Order 12958, as amended, this declaration contains information that may not be released to foreign governments, foreign nationals, or non-U.S. citizens without permission of the originator and in accordance with DNI policy. This information is labeled "NOFORN." The "ORCON" designator means that the originator of the information controls to whom it is released. Finally, this document is marked Manual Review ("MR") indicating that it is not subject to automatic declassification at any specific date.

[3] ~~(S)~~ [redacted]

Approved for public release May 5, 2014

IV. (U) Background Information

A. (U) Background on The National Security Agency

11. (U) The NSA was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense. Under Executive Order 12333, § 1.12(b), as amended, the NSA's cryptologic mission includes three functions: (1) to collect, process, and disseminate signals intelligence (SIGINT) information, of which COMINT is a significant subset, for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c) the support of military operations; (2) to conduct information security activities; and (3) to conduct operations security training for the U.S. Government.

12. ~~(TS//SI)~~ Signals intelligence (SIGINT) consists of three subcategories: (1) communications intelligence (COMINT); (2) electronic intelligence (ELINT); and (3) foreign instrumentation signals intelligence (FISINT). Communications intelligence (COMINT) is defined as "all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients." 18 U.S.C. § 798. COMINT includes information derived from the interception of foreign and international communications, such as voice, facsimile, and computer-to-computer information conveyed via a number of means [redacted] Electronic intelligence (ELINT) is technical intelligence information derived from foreign non-communications electromagnetic radiations except atomic detonation or radioactive sources-in essence, radar systems affiliated with military weapons platforms (*e.g.*, anti-ship) and civilian systems (*e.g.*, shipboard and air traffic control radars). Foreign instrumentation signals intelligence (FISINT) is derived from non-U.S. aerospace surfaces and subsurface systems which may have either military or civilian applications.

Approved for public release May 5, 2014

13. (S) The NSA's SIGINT responsibilities include establishing and operating an effective unified organization to conduct SIGINT activities set forth in Executive Order No. 12333, § 1.12(b), as amended. In performing its SIGINT mission, NSA has developed a sophisticated worldwide SIGINT collection network that acquires, among other things, foreign and international electronic communications and related information. The technological infrastructure that supports the NSA's foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and untold human effort. It relies on sophisticated collection and processing technology.

14. (U) There are two primary reasons for gathering and analyzing foreign intelligence information. The first, and most important, is to gain information required to direct U.S. resources as necessary to counter external threats. The second reason is to obtain information necessary to the formulation of U.S. foreign policy. Foreign intelligence information provided by the NSA is thus relevant to a wide range of important issues, including military order of battle; threat warnings and readiness; arms proliferation; international terrorism; and foreign aspects of international narcotics trafficking.

15. (S) The NSA's ability to produce foreign intelligence information depends on its access to foreign and international electronic communications. Foreign intelligence produced by COMINT activities is an extremely important part of the overall foreign intelligence information available to the United States and is often unobtainable by other means. Public disclosure of either the capability to collect specific communications or the substance of the information derived from such collection itself can easily alert targets to the vulnerability of their communications. Disclosure of even a single communication holds the potential of revealing intelligence collection techniques that are applied against targets around the world. Once alerted,

Approved for public release May 5, 2014

targets can frustrate COMINT collection by using different or new encryption techniques, by disseminating disinformation, or by utilizing a different communications link. Such evasion techniques may inhibit access to the target's communications and therefore deny the United States access to information crucial to the defense of the United States both at home and abroad. COMINT is provided special statutory protection under 18 U.S.C. § 798, which makes it a crime to knowingly disclose to an unauthorized person classified information "concerning the communication intelligence activities of the United States or any foreign government."

B. (U) September 11, 2001 and the al Qaeda Threat.

16. (U) On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial jetliners, each carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Those operatives targeted the Nation's financial center in New York with two of the jetliners, which they deliberately flew into the Twin Towers of the World Trade Center. Al Qaeda targeted the headquarters of the Nation's Armed Forces, the Pentagon, with the third jetliner. Al Qaeda operatives were apparently headed toward Washington, D.C. with the fourth jetliner when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was most evidently the White House or the Capitol, strongly suggesting that al Qaeda's intended mission was to strike a decapitation blow to the Government of the United States—to kill the President, the Vice President, or Members of Congress. The attacks of September 11 resulted in approximately 3,000 deaths—the highest single-day death toll from hostile foreign attacks in the Nation's history. In addition, these attacks shut down air travel in the United States, disrupted the Nation's financial markets and government operations, and caused billions of dollars of damage to the economy.

Approved for public release May 5, 2014

17. (U) On September 14, 2001, the President declared a national emergency "by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States." Proclamation No. 7463, 66 Fed. Reg. 48199 (Sept. 14, 2001). The United States also immediately began plans for a military response directed at al Qaeda's training grounds and haven in Afghanistan. On September 14, 2001, both Houses of Congress passed a Joint Resolution authorizing the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11. Authorization for Use of Military Force, Pub. L. No. 107-40 § 21(a), 115 Stat. 224, 224 (Sept. 18, 2001) ("Cong. Auth."). Congress also expressly acknowledged that the attacks rendered it "necessary and appropriate" for the United States to exercise its right "to protect United States citizens both at home and abroad," and acknowledged in particular that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." *Id.* pmbl.

18. (U) As the President made clear at the time, the attacks of September 11 "created a state of armed conflict." Military Order, § 1(a), 66 Fed. Reg. 57833, 57833 (Nov. 13, 2001). Indeed, shortly after the attacks, NATO took the unprecedented step of invoking article 5 of the North Atlantic Treaty, which provides that an "armed attack against one or more of [the parties] shall be considered an attack against them all." North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246. The President also determined that al Qaeda terrorists "possess both the capability and the intention to undertake further terrorist attacks against the United States that, if not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of the operations of the

Approved for public release May 5, 2014

United States Government," and he concluded that "an extraordinary emergency exists for national defense purposes." Military Order, § 1(c), (g), 66 Fed. Reg. at 57833-34.

19. (U) As a result of the unprecedented attacks of September 11, 2001, the United States found itself immediately propelled into a worldwide war against a network of terrorist groups, centered on and affiliated with al Qaeda, that possesses the evolving capability and intention of inflicting further catastrophic attacks on the United States. That war is continuing today, at home as well as abroad. Moreover, the war against al Qaeda and its allies is a very different kind of war, against a very different enemy, than any other war or enemy the Nation has previously faced. Al Qaeda and its supporters operate not as a traditional nation-state but as a diffuse, decentralized global network of individuals, cells, and loosely associated, often disparate groups, that act sometimes in concert, sometimes independently, and sometimes in the United States, but always in secret—and their mission is to destroy lives and to disrupt a way of life through terrorist acts. Al Qaeda works in the shadows; secrecy is essential to al Qaeda's success in plotting and executing its terrorist attacks.

20. ~~(TS//SI//NF)~~ The *In Camera* Declaration of Michael McConnell, Director of National Intelligence, details the particular facets of the continuing al Qaeda threat and, thus, the exigent need for the NSA intelligence activities described here. The NSA activities are directed at that threat, [redacted]

[redacted]

[redacted]

Global telecommunications networks, especially the Internet, have developed in recent years into a loosely interconnected system—a network of networks—that is ideally suited for the secret communications needs of loosely affiliated terrorist cells. Hundreds of Internet service

Approved for public release May 5, 2014

providers, or "ISPs," and other providers of communications services offer a wide variety of global communications options, often free of charge. [redacted]

21. ~~(TS//SI//NF)~~ [redacted]

22. ~~(TS//SI)~~ Our efforts against al Qaeda and its affiliates therefore present critical challenges for the Nation's communications intelligence capabilities. First, in this new kind of war, more than in any other we have ever faced, communications intelligence is essential to our ability to identify the enemy and to detect and disrupt its plans for further attacks on the United

[4] ~~(TS//SI//OC/NF)~~ [redacted]

Approved for public release May 5, 2014

States. Communications intelligence often is the only means we have to learn the identities of particular individuals who are involved in terrorist activities and the existence of particular terrorist threats. Second, at the same time that communications intelligence is more important than ever, the decentralized, non-hierarchical nature of the enemy and their sophistication in exploiting the agility of modern telecommunications make successful communications intelligence more difficult than ever. It is against this backdrop that the risks presented by this litigation should be assessed, in particular the risks of disclosing particular NSA sources and methods implicated by the claims, [redacted]

[redacted]

V. (U) Information Protected by Privilege

23. (U) As set forth further below, the following categories of information are subject to the DNI's assertion of the state secrets privilege and statutory privilege under the National Security Act, as well as my assertion of the NSA privilege:

A. (U) Information that may tend to confirm or deny whether Verizon/MCI has assisted the NSA with any alleged intelligence activities; and

B. (U) Information that may tend to confirm or deny whether the Plaintiffs have been subject to any of the alleged NSA intelligence activities that may be at issue in this matter; and

C. (U) Information concerning any NSA intelligence, activities, sources, or methods, including:

(1) (U) Information concerning the scope and operation of the Terrorist Surveillance Program, including information that may be needed to demonstrate that the TSP was limited to one-end foreign al Qaeda communications and that the NSA does not otherwise engage in the content surveillance dragnet that the Plaintiffs allege; and

Approved for public release May 5, 2014

(2) (U) Information that would tend to confirm or deny whether the NSA collects large quantities of communication records information as Plaintiffs allege.

VI. (U) Description of Information Subject to Privilege and the Harm of Disclosure

A. (U) Information That May Tend to Confirm or Deny Whether Verizon/MCI Has Assisted the NSA with Any Alleged Intelligence Activities

24. ~~(TS//SI [redacted]//OC/NF)~~ [redacted]

25. ~~(TS//SI [redacted]//OC/NF)~~ [redacted]

[5] ~~(TS//SI [redacted]//OC/NF)~~ [redacted]

Approved for public release May 5, 2014

[redacted]

26. ~~(TS//SI [redacted]//OC/NF)~~ As set forth below, [redacted]

[redacted] Significantly, although Plaintiffs allege that MCI and Verizon have assisted the NSA with a massive, dragnet-type program involving the content surveillance of domestic and international communications made by millions of Americans, such allegations are false. The NSA does not conduct a dragnet of content surveillance of communications made to or from the United States as Plaintiffs allege.

[6] ~~(TS//SI//OC/NF)~~ [redacted]

Approved for public release May 5, 2014

[[Page(s) Redacted]]

Approved for public release May 5, 2014

B. (U) Information That May Tend to Confirm or Deny Whether the Plaintiffs Have Been Subject to Any Alleged NSA Activities That May Be at Issue in This Matter

47. (U) The second major category of information as to which I am supporting the DNI's assertion of privilege, and asserting the NSA's own statutory privilege, concerns information as to whether particular individuals, including the Plaintiffs in the lawsuits against Verizon, have been subject to alleged NSA intelligence activities. As set forth below, confirmation or denial of such information would cause exceptionally grave harm to national security.

1. ~~(TS//SI//TSP//OC/NF)~~ [redacted]

48. ~~(TS//SI//TSP//OC/NF)~~ The named Plaintiffs in this action—which are those listed in paragraphs 24-123 of the Master Consolidated Complaint Against MCI Defendants and Verizon Defendants, as well as those named in the complaints in the *Bready*, *Riordan*, and *Chulsky* actions—allege that the content of their telephone and Internet communications and information related to those communications have been and are being intercepted, disclosed, divulged, and/or used without judicial or other lawful authorization. The NSA does not engage in a program of "dragnet" surveillance that captures the contents of all domestic telephone or Internet communications as Plaintiffs allege, [redacted]

Approved for public release May 5, 2014

[redacted]

2. ~~(TS//SI-[redacted]//OC/NF)~~ [redacted]

49. ~~(TS//SI-[redacted]//OC/NF)~~ [redacted]

[redacted]

[16] ~~(TS//SI//TSP//OC/NF)~~ [redacted]

[17] ~~(TS//SI-[redacted]//OC/NF)~~ [redacted]

Approved for public release May 5, 2014

3. (U) Harm of Disclosure

50. ~~(TS//SI//TSP//OC/NF)~~ [redacted] First, as a matter of course, the NSA cannot publicly confirm or deny whether any individual is subject to the surveillance activities described herein, because to do so would tend to reveal actual targets. For example, if the NSA were to confirm in this case and others that specific individuals are not targets of surveillance, but later refuse to comment (as it would have to) in a case involving an actual target, a person could easily deduce by comparing such responses that the person in the latter case is a target. The harm of revealing targets of foreign intelligence surveillance should be obvious. If an individual knows or suspects he is a target of U.S. intelligence activities, he would naturally tend to alter his behavior to take new precautions against surveillance. [redacted] In addition, revealing who is not a target would indicate who has avoided surveillance and who may be a secure channel for communication. Such information could lead a person, secure in the knowledge that he is not under surveillance, to help a hostile foreign adversary convey information; alternatively, such a person may be unwittingly utilized or even forced to convey information through a secure channel. Revealing which channels are free from surveillance and which are not would also reveal sensitive intelligence methods and thereby could help any adversary evade detection.

Approved for public release May 5, 2014

51. ~~(TS//SI-[redacted]//OC/NF)~~ [redacted]

52. ~~(TS//SI-[redacted]//OC/NF)~~ Disclosing any of this information would reveal some of the Nation's most sensitive and important intelligence-gathering methods. For reasons already discussed, such disclosures would cause exceptionally grave damage to the national security by [redacted] as well as by alerting other foreign adversaries to these critical intelligence-gathering methods. Disclosing whether the NSA currently receives telephony or Internet meta data [redacted] would also violate specific provisions of the FISC Telephone Records and FISC Pen Register Orders.

C. (U) Information Concerning Any NSA Activities, Sources, or Methods, and the Harm of Disclosure.

53. (U) In addition to asserting privilege over whether the NSA has had a relationship with MCI and Verizon in connection with the allegations in this case, and whether the Plaintiffs

Approved for public release May 5, 2014

have been subject to any alleged intelligence activities, I am supporting the DNI's assertion of privilege and asserting the NSA's statutory privilege over any other facts concerning NSA intelligence sources and methods that would be needed to resolve this case. This includes: (1) facts concerning the operation of the Terrorist Surveillance Program and any other NSA intelligence activities needed to demonstrate that the TSP was limited as the President stated to the interception of one-end foreign communications reasonably believed to involve a member or agent of al Qaeda or an affiliated terrorist organization and that the NSA does not otherwise conduct a dragnet of content surveillance as the Plaintiffs allege; and (2) facts that would confirm or deny whether the NSA collects large quantities of communication records information as the Plaintiffs allege. As set forth below, the disclosure of information needed to address these allegations would cause exceptionally grave harm to national security.

1. (U) Information Concerning Plaintiffs' Allegations of Content Surveillance.

54. (U) In December 2005, President Bush explained that, after the September 11 attacks, he authorized the NSA to intercept the content of certain communications for which there are reasonable grounds to believe that (1) such communication originated or terminated outside the United States, and (2) a party to such communication is a member or agent of al Qaeda or an affiliated terrorist organization. The President stated at the time that this activity, now referred to as the Terrorist Surveillance Program, did not involve the collection of purely domestic communications, or international communications with no al Qaeda connection, and these facts were reiterated publicly by the Attorney General and then-Deputy Director of National Intelligence. Nonetheless, I am advised that the Plaintiffs have alleged that the NSA "intercepts millions of communications made or received by people inside the United States, and uses powerful computers to scan their contents for particular names, numbers, words, or

Approved for public release May 5, 2014

phrases." Master Verizon Complaint ¶ 165. As the President made clear in describing the limited scope of the TSP, such allegations of a content surveillance dragnet are false. But if the NSA had to demonstrate in this case that the TSP was limited as the President stated, and not a dragnet as the Plaintiffs claim, and that the NSA does not otherwise engage in the dragnet that Plaintiffs allege, sensitive and classified facts about the operation of the TSP and NSA intelligence activities would have to be disclosed.

55. ~~(TS//SI//TSP//OC/NF)~~ The privileged information that must be protected from disclosure includes the following classified details demonstrating the limited nature of the TSP. First, interception of the content of communications under the TSP was triggered by a range of information, including sensitive foreign intelligence, obtained or derived from various sources indicating that a particular phone number or email address is reasonably believed by the U.S. Intelligence Community to be associated with a member or agent of al Qaeda or an affiliated terrorist organization. Professional intelligence officers at the NSA undertook a careful but expeditious analysis of that information, and considered a number of possible factors, in determining whether it would be appropriate to target a telephone number or email address under the TSP. Those factors included whether the target phone number or email address was: (1) reasonably believed by the U.S. Intelligence Community, based on other authorized collection activities or other law enforcement or intelligence sources, to be used by a member or agent of al Qaeda or an affiliated terrorist organization; [redacted]

Approved for public release May 5, 2014

[redacted]

56. ~~(TS//SI//TSP//OC/NF)~~ Once the NSA determined that there were reasonable grounds to believe that the target is a member or agent of al Qaeda or an affiliated terrorist organization, the NSA took steps to focus the interception on the specific al Qaeda-related target and on communications of that target that are to or from a foreign country. In this respect, the NSA's collection efforts were [redacted] that the NSA had reasonable grounds to believe carry the "one end" foreign communications of members or agents of al Qaeda or affiliated terrorist organizations.

57. ~~(TS//SI-[redacted]//TSP//OC/NF)~~ [redacted]

[redacted]

[18] ~~(TS//SI//TSP//OC/NF)~~ [redacted]

[redacted]

Approved for public release May 5, 2014

[redacted]

58. ~~(TS//SI-[redacted]//TSP//OC/NF)~~ [redacted]

[redacted]

59. ~~(TS//SI//TSP//OC/NF)~~ The NSA took specific steps in the actual TSP interception process to minimize the risk that the communications of non-targets were intercepted. With respect to telephone communications, specific telephone numbers identified through the analysis outlined above were [redacted] so that the only communications

Approved for public release May 5, 2014

intercepted were those to or from the targeted number of an individual who was reasonably believed to be a member or agent of al Qaeda or an affiliated terrorist organization. For Internet communications, the NSA used identifying information obtained through its analysis of the target, such as email addresses [redacted] to target for collection the communications of individuals reasonably believed to be members or agents of al Qaeda or an affiliated terrorist organization.[19]

60. ~~(TS//SI//TSP//OC/NF)~~ In addition to procedures designed to ensure that the TSP was limited to the international communications of al Qaeda members and affiliates, the NSA also took additional steps to ensure that the privacy rights of U.S. persons were protected. [redacted]

[19] ~~(TS//SI [redacted]//TSP//OC/NF)~~ [redacted] At no point did the NSA search the content of the communications [redacted] with "key words" other than the targeted selectors themselves. Rather, the NSA targeted for collection only email addresses [redacted] associated with suspected members or agents of al Qaeda or affiliated terrorist organizations, or communications in which such [redacted] were mentioned. In addition, due to technical limitations of the hardware and software currently used, incidental collection of non-target communications has occurred, and in such circumstances the NSA applies its minimization procedures to ensure that communications of non-targets are not disseminated. To the extent such facts would be necessary to dispel Plaintiffs' erroneous dragnet allegations, they could not be disclosed without revealing highly sensitive intelligence methods.

Approved for public release May 5, 2014

[redacted]

61. ~~(TS//SI//TSP//OC/NF)~~ [redacted]

62. ~~(TS//SI//TSP//OC/NF)~~ In addition to these facts about the TSP, facts about other NSA intelligence activities would be needed to explain or prove that the NSA does not conduct a

---

[20] ~~(U//FOUO)~~ In addition, in implementing the TSP, the NSA applied the existing Legal Compliance and Minimization Procedures applicable to U.S. persons to the extent not inconsistent with the President's authorization. *See* United States Signals Intelligence Directive (USSID) 18. These procedures require that the NSA refrain from intentionally acquiring the communications of U.S. persons who are not the targets of its surveillance activities, that it destroy upon recognition any communications solely between or among persons in the U.S. that it inadvertently acquires, and that it refrain from identifying U.S. persons in its intelligence reports unless a senior NSA official determines that the recipient of the report requires such information in order to perform a lawful function assigned to it and the identity of the U.S. person is necessary to understand the foreign intelligence or to assess its significance.

Approved for public release May 5, 2014

dragnet as Plaintiffs allege. [redacted] None of these activities, however, could be disclosed to address and rebut Plaintiffs' dragnet allegations without causing exceptionally grave damage to the national security.

63. (U) Finally, to the extent the Plaintiffs in this case are challenging the lawfulness of the TSP itself, facts about the operation of that program (which remain highly classified) also could not be disclosed.

64. ~~(TS//SI//TSP//OC/NF)~~ For example, in conjunction with meta data analysis, the TSP provided far greater operational swiftness and effectiveness for identifying the al Qaeda terrorist network in the United States than the traditional procedures that had been used under the Foreign Intelligence Surveillance Act. In order to ascertain as rapidly as possible the potential al Qaeda terrorist threats facing the United States, the NSA must know not only what a foreign terrorist target says in a particular telephone or Internet intercept, but with whom that person has been communicating. To the extent individual court orders for all TSP targets could have been required in advance under traditional FISA procedures, the NSA would have been unable to target communications sent to and from new phone numbers or Internet accounts as quickly, and valuable intelligence could have been lost.

Approved for public release May 5, 2014

65. ~~(TS//SI//TSP//OC/NF)~~ As noted, [redacted] the TSP, in conjunction with meta data collection and analysis, allowed the NSA to obtain rapidly not only the content of a particular communication, but connections between that target and others who may form a web of al Qaeda conspirators. In some cases, the NSA was able to begin collection on a target phone number in [redacted] to begin collection on a targeted phone number or email address. In contrast, if individual applications have to be prepared and approved through the traditional FISA process before the NSA can target a newly identified phone number or email account associated with al Qaeda, vital information could be lost in the interim. The traditional FISA process is a highly effective tool for many types of surveillance activities, [redacted] it would have had to stop and demonstrate, through a multi-layered process involving NSA and DOJ counsel, the Attorney General, and the FISA Court, that each of numerous, [redacted] target numbers or emails requires coverage. Where the gravest of dangers are at stake—a catastrophic mass casualty terrorist attack against the U.S. Homeland and the corresponding need to track thousands of potential terrorists—and where [redacted]

[21] ~~(TS//SI//TSP//OC/NF)~~ [redacted]

Approved for public release May 5, 2014

[redacted] to hide their communications and tracks, it is vital that the NSA be able to track multiple communications, contacts, and [redacted] as rapidly as possible to fulfill its mission to protect the national security of the United States.

66. ~~(TS//SI//TSP//OC/NF)~~ None of the foregoing information about the Terrorist Surveillance Program could be disclosed in this case, however, without causing exceptionally grave harm to the national security. Even though the President has determined not to reauthorize the TSP, revealing how the program operated would provide key insights to foreign adversaries as to how the NSA monitors communications. Information about the specific foreign intelligence factors that triggered interception under the TSP would obviously reveal to foreign adversaries the very facts that would most likely lead to their communications being intercepted, even under the current FISA Court Orders, thereby giving adversaries a roadmap as to how to avoid such interception. [redacted]

67. ~~(TS//SI//TSP//OC/NF)~~ Likewise, information about the speed and agility with which the NSA can collect content on a target, and how long it might maintain surveillance, would provide invaluable insights for an adversary to devise new and different ways to protect their communications. In particular, disclosure of the NSA's ability to utilize the TSP (or, therefore, the current FISA Court-authorizes content collection) in conjunction with contact chaining [redacted] would severely undermine efforts to detect terrorist activities. Armed with this knowledge, an adversary could make more robust use [redacted] Also, as noted, [redacted]

Approved for public release May 5, 2014

[redacted] Compromise of one NSA method of surveillance, even no longer in use, can easily lead to evasive actions as to other current methods that would deprive U.S. decision-makers of critical information needed to detect al Qaeda terrorist threats.

2. ~~(TS//SI-[redacted]//OC/NF)~~ Information Concerning Meta Data Activities

68. **(U)** I am advised that this lawsuit also puts at issue allegations concerning whether the NSA has acquired large quantities of communication records. Confirmation or denial of any information concerning these particular allegations, however, will cause exceptionally grave damage to the national security.

69. ~~(TS//SI-[redacted]//OC/NF)~~ As noted above, starting in October 2001, and now pursuant to the FISC Pen Register Order, [redacted] pursuant to the FISC Telephone Records Order, [redacted] Disclosure of the NSA's meta data collection activities, either before or after FISC authorization, would cause exceptionally grave harm to national security.

70. ~~(TS//SI-[redacted]//OC/NF)~~ In particular, the bulk collection of Internet and telephony meta data allows the NSA to use critical and unique analytical capabilities to track the

Approved for public release May 5, 2014

contacts [redacted] of members or agents of [redacted] through the use of two highly sophisticated tools known as "contact chaining" and [redacted] Contact-chaining allows the NSA to identify telephone numbers and email addresses that have been in contact with known [redacted] numbers and addresses; in turn, those contacts can be targeted for immediate query and analysis as new [redacted] numbers and addresses are identified. Obtaining the meta data [redacted] in bulk, moreover, allows the NSA not only to track the contacts made by a particular telephone number or email address from a certain point in time going forward, but also to trace historically the contacts made with that number or address. This tool has been highly useful in detecting previously unknown terrorist operatives or agents for further surveillance.

71. ~~(TS//SI [redacted]//OC/NF)~~ [redacted]

72. ~~(TS//SI [redacted]//OC/NF)~~ [redacted]

Approved for public release May 5, 2014

[redacted]

73. ~~(TS//SI//TSP//OC//NF)~~ The capability provided by meta data analysis may be illustrated by an example of when this tool was not utilized. According to the 9/11 Commission report, when Khalid al-Mihdhar, one of the 9/11 hijackers, was in the United States from January 2000 to June 2001, he telephoned the home of his wife's family in Yemen. The phone number for this home in Yemen had well-established terrorist connections[22] and was being targeted by the NSA through an overseas collection process that did not have the capability to obtain meta data to help identify the location of incoming calls. At the time, there was no FISA collection on this number, and neither the TSP program, under which the NSA targeted one-end foreign calls

[22] ~~(TS//SI//NF)~~ In August 1998, the number was found in the pocket of one of the would-be Kenyan Embassy bombers, who had fled the bomb-ladened vehicle at the last minute. [redacted]

Approved for public release May 5, 2014

into the United States, nor collection of bulk meta data that would have allowed analysis of this number to ascertain other contact numbers, were in place. Had the Yemeni phone number been targeted using the TSP and were meta data analysis available, we should have been able to identify that al-Mihdhar was in the United States when he called the number in Yemen, which would have provided leads to investigate the matter further. Indeed, the 9/11 Commission report noted that if the FBI had known that al Mihdhar was in the United States, "investigations or interrogation of [al Mihdhar], and investigation of [his] travel and financial activities could have yielded evidence of connections to other participants in the 9/11 plot. The simple fact of [his] detention could have derailed the plan. In any case, the opportunity did not arise." Final Report of the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission Report") at 272. While there is an element of hindsight to this example, and perhaps other actions could have detected al Mihdhar, the existence of the TSP and meta data activities would have provided a highly significant tool that may have proved valuable in detecting the 9/11 plot.

74. ~~(TS//SI//TSP//OC/NF)~~ Based on my experience as Director of the NSA, I believe that the meta data collection activities authorized by the President after 9/11 and subsequently authorized by the FISC are among the most important intelligence tools available to the United States for protecting the Homeland from another catastrophic terrorist attack. In my view, the NSA could not have obtained certain critical intelligence in any other way. These NSA activities have given the United States unparalleled ability to understand [redacted] If employed on a sufficient volume of raw data, contact chaining [redacted] can expose [redacted] and contacts that were previously unknown. Meta data collection thus enables the NSA to segregate some of that very small amount of otherwise undetectable but highly valuable information from the overwhelming

Approved for public release May 5, 2014

amount of other information that has no intelligence value whatsoever—in colloquial terms, to find at least some of the needles hidden in the haystack. [redacted]

Disclosure or confirmation of the NSA's bulk collection and targeted analysis of telephony meta data would confirm to all of our foreign adversaries [redacted] the existence of these critical intelligence capabilities and thereby severely undermine NSA's ability to gather information concerning terrorist connections.

3. ~~(TS//SI//TSP//OC/NF)~~ Information Demonstrating the Success of the TSP and Meta Data Activities.

75. ~~(TS//SI//TSP//OC/NF)~~ Specific examples of how the TSP, in conjunction with meta data analysis, led to the development by the NSA of actionable intelligence and important counter-terrorism efforts help illustrate the effectiveness and need for the program, but could not be disclosed without revealing specific NSA intelligence information, sources, and methods. For example:

Approved for public release May 5, 2014

A. ~~(TS//SI//TSP//OC/NF)~~ [redacted]

[redacted]

Approved for public release May 5, 2014

[redacted]

B. ~~(TS//SI//TSP//OC/NF)~~ [redacted]

[redacted]

C. ~~(TS//SI//TSP//OC/NF)~~ [redacted]

[redacted]

Approved for public release May 5, 2014

[redacted]

D. ~~(TS//SI//TSP//OC/NF)~~ [redacted]

[redacted]

E. ~~(TS//SI//TSP//OC/NF)~~ [redacted]

[redacted]

Approved for public release May 5, 2014

[redacted]

F. ~~(TSP//SI/TSP//OC/NF)~~ [redacted]

[redacted]

G. ~~(TS//SI/TSP//OC/NF)~~ [redacted]

[redacted]

H. ~~(TS//SI//TSP//OC/NF)~~ [redacted]

[redacted]

Approved for public release May 5, 2014

[redacted]

I. ~~(TS//SI//TSP//OC/NF)~~ [redacted]

[redacted]

J. ~~(TS//SI//TSP//OC/NF)~~ [redacted]

[redacted]

76. ~~(TS//SI//TSP//OC/NF)~~ Information about any of the successes of NSA activities would not only be revealing of the substantive knowledge of the United States Government as to

Approved for public release May 5, 2014

terrorist plans and activities, but would also tend to reveal or confirm to all of our foreign adversaries the sources and methods by which the United States obtained such information.

4. ~~(TS//SI//OC/NF)~~ Information Concerning FISC Orders.

77. ~~(TS//SI//TSP//OC//NF)~~ Information concerning the various orders of the Foreign Intelligence Surveillance Court mentioned throughout this declaration must remain protected from public disclosure. As discussed above, the three relevant NSA intelligence activities authorized by the President after the September 11 attacks to detect and prevent a further al Qaeda attack—the TSP, Internet meta data collection, and telephony meta data collection—have been subject to various orders of the FISC and are no longer being conducted under Presidential authorization. The very existence of the meta data FISC orders—the FISC Pen Register Order (first issued in July 2004) and the FISC Telephone Records Order (first issued in May 2006)—remains classified. The President authorized the disclosure of the general existence of the January 10, 2007 FISC orders that authorized electronic surveillance of [redacted] individuals in a manner similar to that undertaken in the TSP, and President's authorization of the TSP lapsed in February 2007. Information that may reveal the existence of the undisclosed FISC orders or the substance of any of these orders should be protected from disclosure.

78. ~~(TS//SI-[redacted]//OC//NF)~~ Disclosure of information about and within the FISC orders would obviously reveal intelligence sources and methods currently being utilized by the NSA under Court order and, thus, would cause exceptional harm to national security. For example, as discussed above, the FISC Telephone Records Order requires [redacted] and authorizes the NSA to access its archive of collected telephony meta data only when the NSA has identified a known telephone number reasonably suspected to be associated with [redacted]

Approved for public release May 5, 2014

[redacted]. The Order also provides that a telephone number believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment. The FISC Pen Register Order authorizes the use of a pen register and trap and trace device to collect Internet meta data [redacted] on similar terms. Disclosure of these facts would reveal sensitive sources and methods utilized by the NSA to obtain data utilized to track [redacted] and contacts of [redacted][23]

79. ~~(TS//SI//OC//NF)~~ The intelligence activities authorized by the FISC Pen Register and FISC Telephone Records Orders must not be compromised by the disclosure of other information. For example, as discussed above, the disclosure of [redacted] Thus, any attempt to address the lawfulness of the meta data activities under Presidential authorization prior to the FISC orders could not disclose, or risk disclosure of, current NSA operations under FISC Orders.

---

[23] ~~(TS//SI-[redacted]//OC//NF)~~ For this reason, the FISC Telephone Records Order and FISC Pen Register Orders prohibit any person, [redacted] from disclosing to any other person that the NSA has sought or obtained the telephony meta data, other than to (a) those persons to whom disclosure is necessary to comply with the Order; (b) an attorney to obtain legal advice or assistance with respect to the production of meta data in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. The FISC Orders further provide that any person to whom disclosure is made pursuant to (a), (b), or (c) shall be subject to the nondisclosure requirements applicable to a person to whom the Order is directed in the same manner as such person. [redacted]

Approved for public release May 5, 2014

80. ~~(TS//SI//OC//NF)~~ The disclosure of information concerning the recent FISC Orders authorizing electronic surveillance would also harm national security. The January 10, 2007 Foreign Telephone and Email Order authorized, among other things, electronic surveillance of telephone and Internet communications [redacted] when the Government determines that there is probable cause to believe that (1) one of the communicants is a member or agent [redacted] and (2) the communication is to or from a foreign country, *i.e.*, a one-end foreign communication to or from the United States.[24] The telephone numbers and email addresses to be targeted (*i.e.*, "selectors") under this order were further limited to those that the NSA reasonably believes are being used by persons *outside* the United States. Under the order, every 30 days the Government is required to submit a report to the FISA Court listing new selectors that the NSA has targeted during the previous 30 days and briefly summarizing the basis for the NSA's determination that the probable cause standard has been met.

81. ~~(TS//SI//OC//NF)~~ The surveillance under this new FISA Court Foreign Telephone and Email Order, which is subject to detailed minimization and oversight procedures, was authorized for 90 days and indicated that it may be reauthorized by the FISA Court upon application by the Attorney General. The order states that, with each request for reauthorization, the Government is required to present a list of current selectors previously reported to the FISA Court that the Government intends to continue to task for collection under the reauthorization. The order further indicated that, at any time, the FISA Court may request additional information regarding particular selectors, and, if the Court finds that the applicable probable cause standard

[24] ~~(TS//SI//TSP//OC//NF)~~ [redacted] That fact, which is not relevant to this action, is, like the other details in the orders, highly classified.

Approved for public release May 5, 2014

is not met, it may direct that the surveillance under the order shall cease on the selector(s) in question. The innovation of this order was that it allowed the Government to target for collection communications related to new [redacted] selectors used by terrorists without having to seek advance approval from the FISA Court for each individual selector. Upon the initiation of the surveillance authorized under the Foreign Telephone and Email Order, the NSA monitored over [redacted] foreign selectors. [redacted] the reporting of these initial selectors occurred over a 90-day period.

82. ~~(TS//SI//TSP//OC//NF)~~ [redacted]

[redacted]

[25] ~~(TS//SI//OC//NF)~~ [redacted]

Approved for public release May 5, 2014

[redacted] While the general existence of the January 2007 orders, as described publicly by the Attorney General, is not classified, the number, nature, and contents of the specific orders described herein are highly classified. Among other things, disclosing to our enemies what surveillance activities, targets and methods are or are not covered by FISA Court orders would reveal sources and methods of intelligence gathering, and enable the enemy to alter its communications to evade detection.

83. ~~(TS//SI//OC/NF)~~ [redacted] the Government filed applications with the FISA Court to renew for 90 days the surveillance authority granted by the FISA Court's January 10 orders. These applications were considered by a different FISA Court Judge based on the FISA Court's typical assignment practice. By order [redacted] the FISA Court [redacted] The Court, however, did not grant the Government's application to renew the surveillance authority in the Foreign Telephone and Email Order (concerning surveillance targeting telephone numbers and e-mail addresses reasonably believed to be used by persons outside the United States). Rather, it issued an Order and Memorandum opinion on April 3, 2007, declining to adopt the interpretation of the Foreign Intelligence Surveillance Act underlying the Government's application for the Foreign Telephone and Email Order. The Court

---

[26] ~~(TS//SI//OC//NF)~~ [redacted] it plans to do so by a process in which it will obtain authorization of the FISA Court for each individual selector.

Approved for public release May 5, 2014

nevertheless ordered that the Government could submit an application for a single extension of the Foreign Telephone and Email Order to May 31, 2007. The Court contemplated that an extension of surveillance authority to May 31 would allow the Government to submit an application that might permit the Court "to authorize at least part of the [requested] surveillance in a manner consistent with [its] order and opinion." On the Government's application, the Court granted a separate order issued on April 5, 2007, extending the surveillance authority granted by the Foreign Telephone and Email Order to May 31, 2007.

84. ~~(TS//SI//OC//NF)~~ The Government is reviewing the new FISA Court orders and intends to work with the FISA Court in the hopes of developing an approach for continuing the authorized surveillance beyond May 31, 2007, in a manner consistent with the April 3, 2007, order of the FISA Court. The details of these orders, and targets implicated by the orders, like the operational details and targets of the ongoing FISA Court-approved surveillance, are highly classified. Thus, information about the nature of these recent FISC orders should not be disclosed in this case.

Approved for public release May 5, 2014

VII. (U) Risks of Allowing Litigation to Proceed

85. ~~(TS//SI-[redacted]//OC/NF)~~ Upon examination of the allegations, claims, facts, and issues raised by this case, it is my judgment that sensitive state secrets are so central to the subject matter of the litigation that any attempt to proceed will substantially risk the disclosure of the privileged state secrets described above. This case directly implicates the conduct of highly classified NSA intelligence activities. Those activities are not peripheral to the case: they are the very subject of this lawsuit. In my judgment, any effort to probe the outer-bounds of classified information would pose inherent and significant risks of the disclosure of classified information, [redacted]

86. ~~(TS//SI-[redacted]//OC/NF)~~ Indeed, any effort merely to allude to those facts in a non-classified fashion could be revealing of classified details that should not be disclosed. As noted, even seemingly minor or innocuous facts, in the context of this case or other non-classified information, can tend to reveal, particularly to sophisticated foreign adversaries, a [redacted] of U.S. intelligence gathering sources and methods.

87. ~~(TS//SI-[redacted]//OC/NF)~~ [redacted]

VIII. (U) Summary and Conclusion

88. ~~(TS//SI//NF)~~ The United States has an overwhelming interest in detecting and thwarting further mass casualty attacks by al Qaeda. The United States has already suffered one attack that killed thousands, disrupted the Nation's financial center for days, and successfully

Approved for public release May 5, 2014

struck at the command and control center for the Nation's military. Al Qaeda continues to possess the ability and clear, stated intent to carry out a massive attack in the United States that could result in a significant loss of life, as well as have a devastating impact on the U.S. economy. According to the most recent intelligence analysis, attacking the U.S. Homeland remains one of al Qaeda's top operational priorities, *see In Camera* Declaration of Michael McConnell, DNI, and al Qaeda will keep trying for high-impact attacks as long as its central command structure is functioning and affiliated groups are capable of furthering its interests.

89. ~~(TS//SI//NF)~~ Al Qaeda seeks to use our own communications infrastructure against us as they secretly attempt to infiltrate agents into the United States, waiting to attack at a time of their choosing. One of the greatest challenges the United States confronts in the ongoing effort to prevent another catastrophic terrorist attack against the Homeland is the critical need to gather intelligence quickly and effectively. Time is of the essence in preventing terrorist attacks, and the government faces significant obstacles in finding and tracking agents of al Qaeda as they manipulate modern technology in an attempt to communicate while remaining undetected. The NSA activities described herein are vital tools in this effort.

90. ~~(TS//SI//NF)~~ For the foregoing reasons, in my judgment the disclosure of the information at issue in this lawsuit would cause exceptionally grave damage to the national security of the United States. In addition to upholding the state secrets privilege and statutory privilege assertions by the Director of National Intelligence in this case, I request that the Court also uphold my assertion of NSA's statutory privilege to protect information about NSA activities. Finally, it is my view that continued litigation of this lawsuit, which directly puts at issue highly classified NSA intelligence activities [redacted] would risk the disclosure of sensitive classified information and,

Approved for public release May 5, 2014

accordingly, that the Court should not only protect from disclosure the classified information described herein but dismiss this lawsuit.

I declare under penalty of perjury that the foregoing is true and correct.

DATE: 20 APR 07

LT. GEN. KEITH B. ALEXANDER
Director, National Security Agency